PRIVACY IN THE COMMERCIAL WORLD

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MARCH 1, 2001

Serial No. 107–16

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

71–496PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

PRIVACY IN THE COMMERCIAL WORLD

THURSDAY, MARCH 1, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m. in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Upton, Shimkus, Bryant, Buyer, Terry, Tauzin (ex officio), DeGette, Doyle, John, Harman, Markey, Gordon, Rush, Eshoo, and Dingell (ex officio).

Staff present: Ramsen Betfarhad, majority counsel; Yong Choe, majority clerk; Bruce Gwinn, minority professional staff; and Courtney Johnson, minority clerk.

Mr. STEARNS. The subcommittee will come to order. I want to thank all of you for attending this morning the first hearing of the Subcommittee on Commerce, Trade, and Consumer Protection. In particular, I would like to thank Diana DeGette from Colorado, who is substituting for Eddie Towns, who had to go back to New York City. And I want to thank, of course, all of the members of the subcommittee.

I want to thank, of course, our distinguished witnesses for appearing before this panel, and I look forward to their testimony and hearing their answers to our questions.

I plan on and expect that this subcommittee, all of us working together, will create a productive and distinguished record for the 107th Session. I look forward to working with each and every subcommittee member.

The subcommittee's jurisdiction is broad and encompasses areas which pose some difficult and complicated questions. Privacy is just one such question. I'd like to take a moment to briefly outline my priorities for this subcommittee. They are, one, privacy and other e-commerce issues; two, international trade, specifically as it relates to e-commerce; and three, discrete consumer protection issues, such as continued work on tire safety, car safety; and, four, these mega-mergers that we see today.

The subcommittee is the front-line subcommittee on the topical issue of privacy. We, I believe, must create a forum for open and honest discussion on the subject. Moreover, I think the subcommittee must also advance the cause of e-commerce by examining and, if need be, addressing some of the more significant issues confronting e-commerce, both at home and abroad.

The international dimensions of e-commerce will be another focal point of our subcommittee's actions. Developments beyond our shores, in particular in the European Community, relating to e-commerce necessitate our careful examination and heightened vigilance on the matter. Finally, there are a myriad of consumer protection issues that we will pursue.

Today, we begin to address what may be one of the most difficult and important issues confronting Congress this session. That issue is information privacy in the commercial world. Today's hearing is the first in a series addressing the issue of information privacy. I believe it is incumbent upon us to create a forum for open and honest discussion.

Precisely for these reasons, we must ask today's witnesses, a distinguished group of scholars and thinkers on the matter, to place the issue in its proper historical context. It is rare that you have a hearing without legislation in place. And so, today, I seek to establish this forum to have the proper historical, intellectual and jurisprudential contexts before we even begin.

We must raise the fundamental issues that are implicated in this discussion. It would not be an understatement to suggest that information privacy in the commercial context is a complex and indeed a vexing issue. The testimony today will attest to its complexity, scope and breadth. For example, the issue of privacy transverses such varied areas of common law as contracts, torts and property, and information privacy as it relates to commercial activities carries with it an implication well beyond the world of commerce.

Today, we will hear testimony advising us to be vigilant and careful when contemplating information privacy fixes for the commercial world, for we may risk triggering serious Constitutional questions and violations. In addressing the issue of information privacy, we must be mindful of the First Amendment, a cornerstone of the American democracy. The testimony also informs us of the tremendous benefits that have accrued to our economy and the American consumer from the tradition of a free flow of information within the commercial context, and we are warned of the negative repercussions that attach to a restrictive information regime in the commercial world. On the other hand, we must also be advised that information privacy rights have enabled the development of new commercial services.

I have highlighted just a few interesting observations extrapolated from today's testimony. There are many more, my colleagues. But today's testimonies are a testimony to the richness and complexity of the debate we as a subcommittee are embarking upon this morning. So I encourage all members to take the time to carefully examine the issues before us, and I hope you will find, as I am sure you will, this hearing helpful as we move this process forward.

In closing, I would like to reiterate my commitment to having a close working relationship with all subcommittee members. I look forward to bipartisanship and a willingness to put together legislation that is meaningful.

With that, I will call upon Ms. DeGette for her opening statement.

Ms. DEGETTE. Thank you, Mr. Chairman.

Mr. Chairman, I was privileged to work with Mr. Towns on the previous Financial Services Subcommittee and know I can speak for both of us in saying that all of the members of the minority, particularly myself and Mr. Towns, look forward to working with you on these important issues of privacy. I want to commend you for quickly holding this first hearing on the topic. I know it is a very complex topic, and those pesky little Constitutional issues do creep up. I am glad that you recognize that, too.

We all know that it is an important subject and one that needs to be addressed. I also want to welcome the witnesses here today. I know I speak for all of the members in saying we look forward to hearing your testimony.

Over the past few years, my constituents have become more and more interested and concerned about personal privacy protections. I personally believe that the diversity of views among different industries and consumer groups, coupled with the complexity of the issue, will make it a very challenging task for policymakers. However, I think that there is a consensus that we need to address both the perceived and real fears that people have with respect to their privacy, particularly in this electronic age.

As I mentioned, I was on the Financial Services Subcommittee and was privileged to be a conferee on the Gramm-Leach-Bliley legislation that overhauled the financial services industry. Privacy was a big issue during those negotiations. Some think that the final language was a good compromise; some think it went too far; and many think it didn't go far enough.

One thing everyone has an agreement on: it was no easy feat to try to strike a balance between preserving the competitiveness of business and protecting the privacy of consumers. I think that that is an issue that the Federal legislators will struggle with for many years to come. I do think, though, that there are two dirty little secrets in the context of this issue. The first is privacy can actually be good for business. The second is information sharing can actually be good for consumers.

Certainly, the issue of privacy can be a new opportunity for increased consumer confidence and trust in business. I know there are many companies that are already busily working customers with their own privacy policies. Every consumer who participates in the new economy has privacy concerns on one level or another, and I know that everyone will work together who has a stake in privacy issues to ensure that the rights and responsibilities of consumers are balanced with that of business.

Privacy should and needs to be at the top of every company's priority list. It should be noted that more than one expert on this topic has called privacy not just a social or moral issue but the single most important business decision a company can make today. And I want to talk just a moment about medical privacy. Congress acted in a bipartisan fashion in 1996 when it mandated that a sweeping medical records privacy bill be passed by 1999. The goal was not met, and as everyone here knows, the Clinton administration wrote the new HIPAA regulations at the end of last year.

I have heard from many constituents back home who are in the health care industry that these new regulations are too burden-

some, and the bar has been set too high. I am sympathetic with those concerns, but I do believe that the administration needs to work with this subcommittee and the rest of Congress to modify the regulations rather than simply withdrawing them, because I do believe that medical records privacy is a critical issue.

Mr. Chairman, again, I look forward to hearing from the witnesses today, and I particularly look forward to working with you and the rest of these members on these complex issues over the next 2 years.

Mr. STEARNS. Thank you.

And now, we have our distinguished chairman of the committee here for his opening statement. Mr. Chairman?

Mr. TAUZIN. Thank you, Mr. Chairman. Good morning.

I want to welcome everyone here today, especially the panel of witnesses. I remember when I first entered the Louisiana legislature, Cliff, and I had my first chance to examine my own law professors——

What a wonderful experience that was to be able to ask them a few tough questions for a change.

I want to also acknowledge to all of you: this is the first official action of the Subcommittee on Commerce, Trade, and Consumer Protection, and I particularly want to welcome Chairman Stearns to this endeavor. This committee is going to be an extremely busy committee this year, and information privacy is obviously one of many big concerns of this committee, but it is a huge one, and I want to congratulate you, Cliff, for making it the first inquiry of this session.

I also want to welcome two members who are not here now, but your ranking member, Mr. Towns, who has been a dear friend for a long time, and he and the vice-chairman of the committee, Deal, are going to be great assets to you as you move forward with this and other hearings, and I want to wish you all well, particularly the new members of the subcommittee, as they are new members of the committee. This issue is particularly intriguing, and I am glad you are starting with an examination of the legal foundations, philosophical basis. We need to think through what privacy has meant in this country and how it has been applied in the context of the various jurisdictions and the U.S. Constitution. Hearing from professors who have thought about, written about and understand many of the complex issues is a good start. I want to thank you for that.

But I also want to point out, as did Ms. DeGette, that this is not a new issue for us. I think if you looked at the books, you would see about 17 statutes on privacy that have been enacted by the Congress over the years: consumer credit—not just the financial services bill and medical privacy but quite a host of smaller but nevertheless important privacy bills that were written in the brick and mortar world to protect people's privacy and, at the same time, protect free speech and the free flow of information. It is a delicate balance.

The other thing I want to point out to you is that while the last administration certainly had a great interest in this subject matter, that we asked the GAO to look at Federal online sites and discovered that the Federal Government was not doing a very good job

of protecting people's privacy, in fact, ironically onsites that people don't necessarily visit voluntarily. For example, the IRS site, which is sort of a site you have got to go to if you don't want to file on paper, and we discovered they even had a cookie on that site.

So we discovered some bad features of our own Federal protection of privacy on Federal Websites, and we need to pay attention, and I know you will look at that, Cliff, as you go forward with these hearings.

I also wanted to point out that every time we have hearings on this, people's positions start shifting. I was just in Silicon Valley the last week or so, and I have seen a different tone. There was a don't do anything attitude for a long time now, and at the conference we had at Landsdowne and meetings I am having lately with folks in the Valley, there is a different attitude. The attitude is you better do something, because we will have 50 states acting and 1,000 other jurisdictions acting, and we will have so many policies and conflict that interstate commerce will get bogged down. And maybe we need to have a common policy that we all understand.

Second, I know you will focus on the great advances made in the private sector, the new self-policing organizations; the new seal of approval organizations, the things that private industry is doing to better inform and give consumers a better chance to protect their own information when they want to. Particularly, I hope you will examine the technological advances that give consumers more security in the information age in regards to information they want to keep private.

And finally, punting might be good in football, but this committee is finished punting. As we meet in this room, downstairs, we are meeting on the Patients First project, a project to deeply involve this committee in the health care issues of this country again. Here on this level, this amazingly complex set of issues that face you, I am excited that you are not punting either. The last thing we ought to do is turn this one over to regulators. We ought to make the policy here. We ought to make it carefully; we ought to make it targeted; we ought to make sure it helps, not impedes, e-commerce. We ought to make sure that when we get through, consumers feel like they are getting a good deal out there, and they have got better control of the information that is pertinent but nevertheless important and sometimes very personal to them.

Mr. Stearns and members of the committee, I want to wish you well. I am delighted, frankly, that you are engaged like this, and Cliff, you know you will have my full support and the support of the entire staff, as I know Mr. Towns will offer his support and his staff to you as well. Good luck and bon voyage.

Mr. STEARNS. Mr. Chairman, thank you for your confidence, and, of course, we look forward to your continued support and your input in this very awe-inspiring attempt to try to come up with a fair, balanced approach that weighs the risk for consumers but also providing the opportunity for technology advancement. So I appreciate your support.

Mr. Dingell, the ranking member of the full committee.

Mr. DINGELL. Thank you, Mr. Chairman.

This is an important hearing, and I commend you for having it. Privacy is not only important to those who don't have it, but it is an essential need of electronic commerce and communication if they are to fulfill their promise. It is not a new issue to this committee. For more than 20 years, we have had privacy provisions for sensitive business information in virtually every major bill that has gone through the committee. For example, in the Safe Drinking Water Act in 1975, the committee gave business strong privacy protections not unlike those advocated today by consumers, Internet users and most of us in our relationships with our health care providers, our financial institutions and our employers.

The act limited information that EPA could collect from business. It also required that EPA give business the ability effectively to opt out or to prevent the agency from publicly releasing sensitive business information. We had a choice to make, and the committee chose to satisfy industry's concerns about sensitive information, so that EPA could get reliable access to the information it needs but not to intrude excessively into the privacy of business or to impair the needs of business to protect business and trade secrets or other matters of concern to business.

Today, individuals need the same kind of assurances that business has gotten and demanded so that the commercial potential of the Internet and the benefits of electronic communication can be fully realized. Without public trust as to the protection of privacy, there will be no ability of business to utilize electronic communications the way they can and should be.

There are a lot of stories about harm that individuals can suffer when privacy is abused today. I would commend to the committee a recent article entitled "Gene Gap Creates New Frontier for Discrimination." This article makes the point that there are strong possibilities that women, for example, who are being examined for breast cancer will refuse to get genetic testing. This has already happened. And their reason, of course, is fear of genetic discrimination;.

There are privacy problems in the financial area, and these are extreme. They are exacerbated by the unfortunate action which the Congress took during the prior session with regard to the financial deregulation legislation that passed last year. Already, we are hearing that there are major problems in banking. Plaintiffs' attorneys now say that fewer than one quarter of the people involved in one case against the Bank of America, the Nation's third-largest bank, have ever been Bank of America customers. But nonetheless, the bank is being sued for having obtained thousands of credit reports and then selling them to entities that were not affiliated with the bank.

So if you want your financial privacy, you better be starting to be concerned about this matter and about the defects and failures, because it appears that the Congress has permitted Pandora to open the box, and the devils which attack privacy are now moving widely through our society. Individuals must have power to control how and when and with whom their personal information is shared. To accomplish this task, the efforts and cooperation of many are going to be needed, and active supervision of this subcommittee and of this committee will be required.

Business is going to have to establish strong self-policing practices and procedures to ensure compliance with privacy guidelines. The Government is going to have to see that honest men are kept honest by a good statutory framework that will punish wrongdoing, which hurts ordinary citizens, and failing that, we can look forward to nothing but trouble in this area.

Mr. Chairman, I look forward to working with you and other members of the subcommittee on this important issue. Thank you.

Mr. STEARNS. I thank you, Mr. Dingell.

Mr. Shimkus, opening statement?

Mr. SHIMKUS. Thank you, Mr. Chairman. I just want to echo what my good friend and colleague Diana DeGette said, and I'm going to use it from now on, Diana. Privacy will be very good for business, and information sharing is and will be found to be very good for the consumer. Marrying those two so that they don't bleed into each other, and we have legal and the Constitutional debate, that is the challenge. That is why you are there to help us, really educate us, on these difficulties. I look forward to hearing your testimony and welcome, and I yield back my time, Mr. Chairman.

Mr. STEARNS. Mr. Doyle?

Mr. DOYLE. Thank you, Mr. Chairman. I want to thank you for convening this hearing to examine individual and consumer privacy protection issues in our growing high-tech economy.

This hearing should provide a forum to address privacy concerns in cyberspace as our Internet and electronic commerce sectors continue to expand and evolve. In recent years, we've witnessed more and more traditional old economy industries and businesses offer their goods and services online, speaking to the fact that e-commerce provides a never-before-seen ease of accessibility and convenience to an increasing volume of consumers.

Newly minted companies immediately turn to the Internet as an effective resource to reach potentially unlimited numbers of customers worldwide. The sudden serve in e-commerce popularity demonstrated a public confidence and willingness to indulge in this innovative medium. Although the recent slowdown in the high-tech and e-commerce industries have created some financial headaches for businesses and investors alike, utilizing the capabilities of the Internet for commerce will remain high on the priority list for competitive industries in the Twenty-First Century.

As more households in America turn to online entities for goods and services, protecting the privacy of users has exploded to the forefront of discussions. In my view, one of the fundamental issues governing the evolution of a thriving high-tech and e-commerce sector in the American economy will be the level of consumer trust in online institutions and communication. Without trust in digital systems and networks, the benefits of this growing economy will be severely limited, and the American public will miss a golden opportunity.

Information privacy concerns are a double-edged sword for e-commerce. Routine information about users and their usage might be used to assist online service providers in government, business and medical areas to provide efficient, informed and highly personalized customer service. Lacking the trust and assurance that their information is truly protected online, consumers will turn away from

online resources. Ensuring consumer trust in online transactions means enhancing online security measures and information sharing practices, thus creating a need for highly trained software and system engineers and companies, spawning more economic growth.

I believe that we in Congress must continue to examine the best means possible to foster and promote sustained economic growth in the high-tech sectors of our economy. Realizing that a critical component of any sustainable growth is high consumer confidence and trust in the available services, we must look at the role the Federal Government must assume to achieve effective results.

I am aware that in the past, far-reaching Federal regulations have created unnecessary burdens on business, to the point where some industries found it economically unfeasible to continue without significant restructuring or downsizing. That is not to say that Federal agencies design to choke firms out of business by promulgating excessive regulations; rather, the Government responded to a definite need to ameliorate certain abusive practices and situations by those industries. But at times, we simply reacted too harshly. It would be unfortunate if a similar situation was to occur with our budding high-tech economy.

In closing, Mr. Chairman, it is my sincere hope that we may find a happy medium from today's discussions in which the privacy and trust of concerned citizens is protected and upheld, while industry practices responsible utilization of consumer information sources as a means to enhance and develop online e-commerce assets.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank my colleague, and I want to welcome one of the newest members to our full committee at Commerce, and I enjoy having him on my subcommittee, Mr. Buyer.

Mr. BUYER. No, I pass.

Mr. STEARNS. Okay.

Mr. BUYER. I want to hear the witnesses.

Mr. STEARNS. Mr. Markey, for an opening statement?

Mr. MARKEY. Thank you, Mr. Chairman very much, and thank you for having this very important hearing today.

We have come a long way in 1 year. A year ago, the industry generally was saying don't tax us; don't force us to give privacy protections; don't pass laws that protect us engaging in fraud, or else, you will ruin the industry. And thank God we didn't do anything on anything, because the industry did it to itself obviously. I will also add another thing: don't expect us to make money or have any revenues, you know.

And the stock market has reflected their view of that. Although it was belated, it obviously has now taken at least half of the air out of that bubble, and so, at least, now, we can discuss these issues without fear that anything we might do in the privacy front would be then responsible for knocking half of the value off of the Nasdaq.

Because obviously, privacy had nothing to do with it. It had to do with the irrational exuberance of those who were investing in the Nasdaq.

So without question, privacy is a looming legislative issue in this Congress. At today's hearing, we can get a brief glimpse of the simmering policy issues that are of increasing concern to Americans

throughout many segments of our society, including financial privacy; Internet privacy; medical privacy and genetic discrimination.

Let me briefly just touch on a few of these issues. With respect to financial privacy, this committee approved legislation which would have given consumers the ability to say no to having their banking, their brokerage or their insurance records shared with affiliates of a huge financial holding company or with third parties. Unfortunately, the House Republican leadership gutted this provision, replacing it with a loophole-ridden privacy provision. We need to close those loopholes so that consumers have control over how their most sensitive financial secrets are disseminated.

With respect to medical privacy, what we have right now is the story of medical privacy on hold. The red light is blinking, but nobody seems to be picking up on the fact that the American people want medical privacy standards. And by law, these protections should have been established a whole year ago. In 1996, Congress promised Americans that specific health privacy protections would be in place by February of 2000. We are over a year late with our promise. I think we have put medical privacy on hold for long enough.

For this reason, I am particularly concerned that the Department of Health and Human Services has recently announced a recent decision to open up the Health Insurance Portability and Accountability Act privacy regulation for a 30-day comment period. I am drafting a letter to be sent to the Secretary, and I hope to get bipartisan support urging the rule's timely implementation.

While this rule isn't perfect, it is a carefully crafted first step toward a comprehensive privacy standard, and once implemented, I plan to introduce legislation to improve it.

With respect to online privacy, it is no secret that I have long been advocating action to put common sense privacy rules on the books to protect privacy in cyberspace. I believe that such action will be good for business, and it will increase consumer confidence in the medium. It is clear that industry self-regulation alone is a failure and is insufficient. Our current policymakes absolutely no sense. It is anti-consumer because it doesn't afford anything remotely resembling comprehensive protections consumers deserve.

Beyond undermining consumer confidence, however, the lack of legal privacy requirements also creates an inverse system of rewards and risks for the industry. If a company posts a privacy policy and then subsequently violates it, the FTC can take action under its authority to police unfair and deceptive practices. Conversely, if a company posts no policy at all and then engages in personal information hijacking, it is legally able to continue on its merry way. The company is shielded by the privacy paradox: as long as it never promises to protect privacy, it can never be accused of deceiving its customers.

Again, I have argued that what we must have is a national privacy policy that continues and urges self-regulatory efforts but complements such efforts with the promotion of technological tools and enhanced privacy as well as a set of meaningful, enforceable privacy guidelines that protect all Americans in the online environment.

I think at this point, everyone is familiar with the essential ingredients of fair information practices. What we need to do now is proceed with a more detailed, rigorous examination of how these principles can be fleshed out legislatively so that beyond our discussion of privacy principles, we can better explain to consumers and industry of how these key privacy rights will work operationally in the online environment.

I encourage both the industry and privacy advocates to articulate in a more detailed fashion what they would like to see in any legislation that this committee considers. I want to commend you, Mr. Chairman. I think we are at the beginning of a very, very important process that I hope will produce, by the end of this year, an online privacy bill of rights that will give every American the protection which they need for their family's secrets.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank my colleague.

Mr. Terry?

Mr. TERRY. I am going to pass, but I want to hear what a privacy bill of rights entails. But I want to flesh out my philosophy on privacy through questions to the panel.

Thank you.

Mr. STEARNS. Ms. Harman for an opening statement?

Ms. HARMAN. Thank you, Mr. Chairman.

One of the primary reasons I sought to join the Energy and Commerce Committee was to serve on this subcommittee, and I am very pleased to see that this subject is first up. I represent a district which 10 years ago was heavily dependent on defense and aerospace. In the last 5 or 10 years, it has transformed itself into the heart of Southern California's digital coast. The new industrial base is e-commerce, multimedia, Web design, telecommunications and other high-tech businesses, and all of them have significant presence in Venice, El Segundo and the South Bay of California.

The success and future of those businesses depends to a large degree on consumer confidence in the Internet, and confidence requires control, giving consumers control over the information that consumers reveal when they are online. How to achieve real consumer control or real consumer choice is tricky, and numbers of our members have just commented on that. I believe that industry self-regulation and code-based solutions like the P3P protocol have a role, but they are probably not the entire answer.

The Federal Government also has a role, and one component of that role needs to be, in my opinion, to preempt some State regulations so that interstate commerce is not impeded. The proliferation of multiple State standards has prompted industry to seek Federal Government help; to seek partnerships. That, in my view, is good, and so is drawing bright lines around personal health and financial records.

Numbers of members this morning have talked about potential abuses. I would just like to mention one real abuse that I learned of last fall while holding hearings on this subject in my district. One woman told me that her husband had been diagnosed with cancer and in this regard was also tested for HIV/AIDS. While he was in the hospital, she happened to sneak a look at his medical

chart which, instead of saying HIV pending, because he had been tested, said HIV positive.

Of course, the test turned out to be negative. She insisted that the chart be changed. But imagine if that information was routinely used by insurance companies, employers or credit card companies. That man's future would have been seriously affected by an inaccurate statement on his medical chart. And so, it is absolutely critical that we find the right ways to protect medical privacy and the related issue of financial privacy.

I am looking forward to this hearing, Mr. Chairman, and to future hearings and to playing as important a role as I can on fashioning a balanced and bipartisan piece of legislation that deals with this critical issue.

Thank you very much.

Mr. STEARNS. I thank my colleague.

Mr. John, opening statement if you have one?

Mr. JOHN. Thank you, Mr. Chairman.

I have a copy of my statement that I would like to submit for the record, and in the interest of time, I would just like to say thank you for this hearing. I think this is very important. And my comments reference, among other things, an article that was in the Wall Street Journal on February 20 that talks about and compares Europe's Web privacy with the United States and how, over the last 5 years, the European Commission has put a wealth of regulations on the books, and they commissioned a study that basically said that there is a balance between what happens in the United States; that self-regulation is not that bad; that some of these regulations have been overburdening, and actually, in the United States, according to the study, there are a lot more privacy protections for consumers without the regulations.

Although I don't think it is absolute, I think it is an interesting read to start us off and to see where we are going and learn from a case study that was actually funded by the EU to learn about privacy and government and private industry's involvement in how you get to that ultimate goal of which I don't think any of us really know or have our finger on, which is consumer protection and also not stifling economic growth.

So I would urge each member of the committee to take a look at this article. It is very interesting. With that, I yield back my time and look forward to the witnesses.

[The prepared statement of Hon. Christopher John and the Wall Street Journal article follow:]

PREPARED STATEMENT OF HON. CHRIS JOHN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF LOUISIANA

Mr. Chairman, thank you for assembling today's panel of experts on privacy matters. I believe that this Subcommittee's focus on privacy will be one of the most important issues that this Congress faces, and I look forward to their testimony.

Mr. Chairman, recent analysis has shown that as goes the NASDAQ, so goes consumer confidence in this country. Granted, these movements have not been rigorously tested statistically, but the point that is relevant to this Subcommittee and this hearing remains: consumer trust and confidence are fundamental to the success of the increasingly global Internet economy and privacy is a critical component of the "trust and confidence" measure that consumers hold. It applies to both e-commerce in general and the practices of specific companies in particular. We have an opportunity during the 107th Congress to ensure that we provide the best environ-

ment for future economic growth while ensuring adequate consumer protections in this regard. I do not believe that these are mutually exclusive goals.

Having said that, I do not have the equation that solves the vexing problem we are dealt here today—resolving American's desire for one-stop shopping on the Internet without making themselves more vulnerable to tracking by criminals, businesses and even the government. However, I would like to submit for the record a recent Wall Street Journal article entitled, "Europe Lags Behind U.S. on Web Privacy." It suggests, via a European consumer's organization study, that Internet users' privacy is better protected in the U.S. than in Europe, despite the privacy directive that exists there. In all fairness, it does not endorse the private sector solution that we have allowed in the U.S. and it is critical of our lack of provisions regarding right to redress. However, I think the lessons and challenges that the article outlines should be paramount on all of our minds as we move forward in discussing privacy matters in this Subcommittee and in this Congress.

Thank you, again, Mr. Chairman for holding this hearing. These matters are of extreme importance to my constituents in the 7th Congressional District of Louisiana. I look forward to the hearing today.

[Tuesday, February 20, 2001—The Wall Street Journal]

EUROPE LAGS BEHIND U.S. ON WEB PRIVACY

MORE AMERICAN FIRMS LET CUSTOMERS GUARD DATA, STUDY FINDS

By Ben Vickers

Internet users' privacy is better protected in the U.S. than in Europe, despite the raft of privacy regulations that have been approved by the European Commission over the past five years, according to European consumers organizations.

The U.S. model of voluntary self-regulation of the use of private data collected online appears to work better, according to a commission-funded study by United Kingdom-based Consumers International, a federation of more than 250 consumer organizations in 110 countries.

The study reveals, for example, that 80% of European Web sites don't comply with current EU law that requires the sites to give online customers the chance to opt out of allowing their personal data to be stored and reused. In the U.S., however, almost 60% of most-popular sites offer their users the chance of opting out of having their data stored and reused.

Fewer sites in Europe collect data on users, compared with the U.S. overall. But of those that do, the study says, only about a third comply with the EU rule on offering public privacy policies. More than 63% of European Web sites collect information on users, but only 32% point them to their privacy policy, which explains that company's use of private data. In the U.S. a massive 90% of sites collect information on users, but 62% of these point users to their privacy policy, according to the study.

"Despite tight EU legislation . . . U.S.-based sites tend to set the standard for decent privacy, policies," the survey of 751 Web sites, concludes.

There are five separate EU Directives that regulate online privacy, plus sections of the European Treaties and Charters, such as the recently finalized European Charter of Fundamental Rights.

Privacy Directive

Two-thirds of the 15 EU-member states have passed the Privacy Directive into their national law. Those who haven't done so yet have until January next year to complete the process. Most of the other directives are already being applied, and some will soon be due for revision.

Each EU member state now has a data-privacy commissioner and a national enforcement agency that monitors compliance with the new laws. But many countries are still adapting their existing agencies to enable them to carry out the work of monitoring the Internet.

And Europe is taking a long time to get around to applying its privacy regulations.

"The evidence is that enforcement [of the regulations] is simply not happening," says Anna Fielder, director of Consumers International in London. "When you talk to the national regulators who are supposed to make sure the rules are applied, they always complain of a lack of funding and a lack of staff for an enormous amount of work," she says.

Although references to the Fundamental Rights and the threat represented by privacy abuses pop up in any parliamentary debate on the privacy issue, the resources for enforcement of privacy rules are not adequate, Consumers International says.

But consumers' organizations, which lobbied hard for the privacy regulations, consider the EU on the right track, despite the lack of enforcement now and the lead the U.S. appears to have in self-regulation.

'A Right to Redress'

"Consumers in the EU have a right to redress. There is a law, there is an enforcement agency in each state . . . Redress in the case of abuse is not available in the U.S. with the voluntary systems they have," says Ms. Fielder. In Europe, consumers have someone who will represent them in the case of a dispute and laws to back up their claims, she says.

At a debate on the need for updating EU privacy regulations last January, Gregory Rohde, the U.S. assistant secretary of commerce for communications and information, told members of the European Parliament that there was a need for "clear, consistent, and enforceable rules."

Mr. Rohde pointed out that while the U.S. has taken very limited action in regulating privacy protection, it has only regulated for financial services, health-care information and for the protection of child privacy online.

"But we are starting to see a shift towards stronger governmental action in the U.S.," Mr. Rohde told members of the European Parliament. "Up to this point, the U.S. has chosen to allow the emerging Internet and new communications systems to develop without broad-scale government regulation," he said.

Online Trading

A focus of the commission's electronic commerce strategy this year is to increase consumer confidence in online trading, according to EU Health and Consumer Protection Commissioner David Byrne. "E-commerce in Europe is being held back by several key worries," Mr. Byrne told European Parliament members. "These are related to the risk of online fraud and data protection."

One solution being encouraged in Europe is a code of conduct and trustmarks—a certification offered by third parties that guarantees minimum standards in areas such as respect of privacy and protection of, personal data. Similar initiatives exist in the U.S., where the private sector has produced third-party verification of privacy policies like Truste (www.truste.org) or Better Business Bureau Online (www.bbb.org). Almost all sites using third-party certification are based in the U.S., according to the commission survey.

The commission says it hopes to encourage their development in Europe. Meanwhile, it has posted a first version of e-commerce "best practices" that resulted from consultations with industry players on its "e-confidence" forum on the Internet, (http://econfidence.jrc.it).

Online consumer-confidence building is also one of the objectives of the recently approved "Brussels Regulation," which allows online consumers to settle disputes in the courts of their country of residence, as is the case for online consumers who are resident in the U.S.

The commission has also recognized the need for introducing credit-card charge-back systems in Europe. Online consumers using credit cards in Europe aren't able to call on card companies to mediate in the case of a dispute with an online supplier, as in the U.S. The charge-back system has given a major boost to the credit-card sector in the U.S., according to Mr. Byrne, who has had contacts with credit-card issuers to look at promoting the system in Europe.

But privacy remains a major concern to online consumers. A survey by American Express Co., covering 10 countries, found 79% of the financial-services company's clients considered privacy and security as major issues in online shopping.

Unwanted E-Mail

The scale of the problem is indicated by the volume of unwanted e-mail dispatched over the Internet. The abuse of private data feeds the turnover of unsolicited e-mail messages, and is expected to cost Internet users 10 billion euros ($9.2 billion) world-wide this year, according to figures just released by the commission, which is also preparing regulations for this area. America Online estimates that one third of the e-mail messages arriving on its servers are unwanted.

The balance between consumer protection and marketplace freedoms that both the EU and the U.S. say they are seeking—though with different approaches—is exemplified in the Safe Harbor certification scheme for U.S. companies willing to Comply with EU Privacy laws in their dealings with EU clients. Companies that don't adhere to the Department of Commerce Plan could find themselves facing court cases in Europe over private-data abuse.

Mr. STEARNS. I thank my colleague, and just for members' information, we have a copy of that study. If anybody on the committee would like it, we would be glad to provide that to them.

Ms. Eshoo?

Ms. ESHOO. Thank you, Mr. Chairman, and as you are talking about copies of things, it might be well for the committee staffs on the majority and minority sides of the aisle to provide for the new members a copy of or summaries of the copies of the testimony of the Federal Trade Commission when they gave testimony in 1999 and then last year before our subcommittee, because it is highly instructive about what they found and how they changed their minds, and I think new members, wherever you land on this, would really benefit for it.

So I would ask for unanimous consent that that be provided for our members.

Mr. STEARNS. I was advised by counsel: this whole thing is on the FTC Website. So, I mean, we are welcome to put this in by unanimous consent, but I think any member, if he or she would like, they can just go on the Website and read it, and they can go back to 1999 and get that testimony.

Ms. ESHOO. What? The testimony that they gave?

Mr. STEARNS. The testimony.

Ms. ESHOO. Good; well, I just wanted to make that suggestion.

Thank you for holding this hearing and for promptly initiating our discussion and a debate on the issue of privacy. The right to privacy is really so highly valued by all Americans. I always say to my staff that I think privacy runs through the veins of the American people. We have a healthy suspicion of government and Big Brother. We don't want anyone and are resentful of anyone ever looking over our shoulders into anything that we believe just belongs to us, to ourselves.

I speak as an American whose privacy I really think was highly violated when, 2 years ago, I found that someone had not only gotten my Social Security number but had filed a fraudulent tax return in my name. So if you don't think that you're vulnerable to something out there, there are stories that can go on and on. And it really brings home very, very quickly what can be done today because of so many of our successes and our breakthroughs relative to technology. But, boy, when it hits the human being, it still has the same effect.

So I think that the Congress is poised today or should be poised today not only in the examination of this issue but also to take the right kind of action. This right that Americans have has evolved through the years of judicial examination and, indeed, civic demand, because again, this is an all-American idea and right.

Now, we are in the midst of the information revolution, and the parameters have certainly changed. We are faced with complex issues, such as finding the correct balance between the protection of our personal information and the level of freedom necessary for the Internet—because the Internet is different—to continue to flourish so that we can continue enjoying its benefits. As both a personal communication tool and as an electronic marketplace for consumers and businesses, the Internet has become a significant

part of the lives of Americans, and it will continue to in a much larger and profound way.

So the privacy of the information that is exchanged is really very, very important to the continued expansion of the Internet. So obviously, we have to find a balance. Members have said that. Balance is a funny word in public policy, because what some people consider to be skewed, other people see it as just right.

In January, January 20, when we had just a very small window of opportunity to introduce legislation, the day the new President was inaugurated, Representative Chris Cannon and myself introduced the Consumer Internet Privacy Enhancement Act. We obviously think that this is a prudent way to go. It establishes a floor, not a ceiling. It mirrors the Kerry-McCain legislation that was introduced in the Senate last year, and I believe the Senators will introduce that mirror legislation again.

Our laws, I believe, need to catch up with and reflect where we are today. They should, in my view, require Website operators to provide clear and conspicuous notice of how they will use personal information. Moreover, consumers should then have the opportunity to make a choice as to whether they want to comply with the operator's stated use of their information. Websites that violate any of these protections should face rigorous penalties, and our bill addresses each of these needs.

Today, for all of the new members, you know this of the committee, it is strictly a voluntary situation. So if someone wants to, fine. Now, the industry, I think, has moved, but the FTC found that there was a need for the Congress to step in. Still, as we protect consumer security, we have to also be sure that we don't legislate an impediment to the free flow of information across the Internet. That is what the Internet is all about. The Consumer Internet Privacy Enhancement Act addresses this factor as well.

I want to just summarize and say, Mr. Chairman, that I look forward to being key in this debate and the shaping of legislation. I don't think there is Republican privacy and Democratic privacy. And I think if there is an area that this Congress can certainly—this subcommittee and our full committee—can come up with is something that consumers will hail and say they got it; they understood it; we now have protections that have some teeth in them. If, in fact, it is necessary to have the teeth to sink in; we also have fully recognized what the Internet represents: the free flow of information without damaging an individual and their privacy.

So with these considerations in mind, I thank you once again, and if I have any time left, I yield it back. And thank you to the witnesses. We have a wealth of information in front of us. So thank you for being here to enlighten us.

Mr. STEARNS. I thank my colleague.

Mr. Gordon?

Mr. GORDON. Thank you, Mr. Chairman.

This is an important issue. I am glad that you have targeted it as a high priority for this subcommittee, and I am confident that if we will work hard and listen to the advice of a lot of folks and try to put that through our system here that we are going to have a good bill that will find Anna's balance. Thank you for this hearing.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you Mr. Chairman for holding this hearing on one of the most important issues under the Subcommittee's jurisdiction—the issue of PRIVACY.

I also want to join my good friend from Florida in welcoming the witnesses on the panel today, and I look forward to hearing their testimony.

Over the past several years, my constituents have become more and more interested and concerned about personal privacy protections. While I personally believe that the diversity of views and the complexity of this issue could make it difficult for us to pass a "one size fits all" policy, I do believe that we need to address the perceived or real fears people have with respect to privacy. Mr. Chairman, I also believe we need to act this Congress in the most deliberate and responsible way possible.

Recently, I read an account in the press where an industry leader said that we in society have no privacy anyway and that we should just "GET OVER IT." That is an unacceptable view in my mind and one that does not sit well with my constituents. Privacy protection is not only very important but very necessary as well.

I would like to encourage my friends who see privacy as a burdensome issue to look at this process as a new opportunity for increased consumer confidence and trust in your businesses. Every consumer who participates in the new economy has privacy concerns on one level or another. I look forward to working with the involved parties to ensure that the rights and responsibilities of consumers are balanced with those of business.

Privacy should and needs to be at the top of every company's priority list. It should be noted that more than one expert on this topic has called privacy not a social or moral issue, but the single most important business decision a company can make today.

We in Congress acted in a bipartisan fashion in 1996 when we mandated that Congress pass a sweeping medical records privacy bill by 1999. This goal was not met and so the Clinton Administration had the responsibility to write the HIPPA regulations at the end of last year. Some in the Healthcare industry have been critical of the new regulations, stating that the bar has been set too high and have lobbied the new administration to re-open the regulation writing process. I believe that this would be a grave mistake in judgment by the administration. People need to be given complete control over their personal medical records and now is not the time to turn back the clock.

In closing, it is critical that we act in moderation as we delve into this issue. I do not want to see premature, knee-jerk legislation pass just so that we can all go home and say we did something that may turn out to be the wrong decision a week, a month or a year from now. If we are going to pass legislation on this issue, lets be sure to get it right—THE FIRST TIME. Again, I look forward to hearing from all of our witnesses today, and I yield back the balance of my time.

PREPARED STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. Chairman, thank you for holding this important hearing on privacy in the commercial world. This subject is extremely far-reaching and complex and I am glad to see that we have such an esteemed panel of experts here before us. However, before turning it over to the panel, I would like to express my concern over one area which seems to be attracting greater and greater attention lately: medical privacy.

As we are all aware, the previous administration issued final regulations last December which would protect the privacy of an individual's medical records from undue intrusion. Those regulations have been re-opened for comment for 30 days by the current administration.

While we may disagree on how to protect the privacy of medical records, I think we can all agree on the over-arching need for medical privacy.

With recent advances in medical technology, such as the mapping of the human genome, it has become increasingly evident that the privacy of one's medical records is the best defense against genetic discrimination. Since we all can agree on the need for medical privacy, I think it is important to discuss how we can obtain that goal without overburdening the health care community responsible for providing care or establishing a system without adequate enforcement mechanisms such as a private right of action. I look forward to working with my colleagues to ensure that

whatever action is taken on the medical privacy regulations, it strikes a balance between operational feasibility for providers and health care facilities and protection of our most sensitive information.

Mr. STEARNS. I thank my colleagues. We are ready for our panel, the first panel we have and only panel. We have Professor Fred Cate, professor of law, Indiana University School of Law; we have Professor Eugene Volokh, professor of law, UCLA School of Law; Professor Paul Rubin, professor of law and economics, Emory University School of Law; Ms. Solveig Singleton, senior policy analyst at the Competitive Enterprise Institute; Mr. Marc Rotenberg, executive director, Electronic Privacy Information Center; and Professor Chai Feldblum, professor of law at Georgetown University Law School.

I welcome all of you here, and we look forward to your opening statements, which, as you understand, are generally 5 minutes.

Professor Cate?

STATEMENTS OF FRED H. CATE, PROFESSOR OF LAW, INDIANA UNIVERSITY SCHOOL OF LAW; EUGENE VOLOKH, PROFESSOR OF LAW, UCLA LAW CENTER; PAUL RUBIN, PROFESSOR OF LAW AND ECONOMICS, EMORY UNIVERSITY SCHOOL OF LAW; SOLVEIG SINGLETON, SENIOR POLICY ANALYST, COMPETITIVE ENTERPRISE INSTITUTE; MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; AND CHAI R. FELDBLUM, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER

Mr. CATE. Thank you very much, Mr. Chairman, members of the committee.

First, let me thank you both for the opportunity to be here but especially for holding a hearing such as this. It is really quite remarkable to have the chance to be part of the hearing where there isn't a particular bill on the table and in an area as complex as privacy in which the ramifications of regulating too much or too little are so great. The opportunity to look at the issue in its entirety, without breaking it into some small subset, some particular area, is particularly appropriate. So I am very grateful for that.

Let me also acknowledge your courage in organizing a panel of primarily law professors, people who, for our very livelihood, never answer a question. This will be an interesting change for us today. In fact, we, of course, normally ask them.

I would like to make just three points today in order to stay within the time limit; first, to talk about the critical roles that information plays in our economy and our society; second, the extent to which privacy laws inevitably are in tension with those roles. Many of you and many other people have noted that they would like privacy laws that did not interfere with the flow of information, and those just don't exist. The question is how you draw that balance, how you balance that tension between the two. And finally, I would like to speak just briefly about some of the limits of consent; that consent is not a way out of this dilemma; consent often, instead, exacerbates this dilemma.

So to start first with what I have called the information infrastructure, it merely recognizes what I believe the Federal Reserve Board and many others have testified before this committee and

others repeatedly: that the accessibility of personal information has created a profound transformation of commerce and the economy in this country. Commerce now depends increasingly on complete, objective and reliable information, and the accessibility, the availability of that information makes it possible to treat consumers as individuals, not as groups. It makes it possible to target services to their specific needs, and it makes it possible to evaluate them for service based on their own records, not on their race or gender or who they know or what they have access to but rather their own demonstrated record in the market.

Now, although I have included in my written testimony numerous examples of this, let me suggest just two now. One is, of course, the whole market for consumer credit, where we see in this country, unlike in Europe, which does have restrictive privacy laws, much wider availability of credit; much faster granting of credit; and much cheaper credit, credit available at much lower costs. This is, of course, because information about consumers is routinely collected, subject to Federal law. It is available so that when a decision needs to be made, it does not have to be put together from scratch; and it is available in a reliable form, so that lenders do not have to insure themselves against bad information or missing information as they do in Europe and therefore charge higher interest rates, fees or other charges.

Now, maybe a second example of this use of information is, of course, the ability to target interested consumers, and you may wonder why anyone in their right mind would ever speak to Congress about what you are certainly going to interpret as junk mail. But the irony is that the argument that information should not be available for targeting marketing opportunities to consumers means not less junk mail but, of course, more and not less satisfying—not more satisfying communications but less, because they will not have been targeted; they will not reflect that consumer's likely interest.

I dare say not one of you here or many people elsewhere in the Congress or in State legislatures have ever run a campaign without contacting people based on knowing what party they belong to; what their likely interest, their likely past donating record has been. This is precisely the type of information that makes it possible to communicate efficiently and effectively with individuals.

Now, against these and many other benefits, we have the privacy tension, the tension that if information is not available or it cannot be used, then it is inevitably going to, as one State attorney general put it, interfere with information flows and cause consumers to pay the price in terms of either higher prices or a restricted set of choices offered to them in the market. This is the inevitable effect of this tension. There is no way around it.

This leads, then, to the third and final point on the limit of consent, because we have heard the argument many times in the privacy debate that all we are seeking in privacy law is that consumers be given a chance to consent. But there are many reasons why consent does not alleviate these concerns; for example, the difficulty of obtaining consent; the difficulty, in many instances, of even reaching consumers, particularly when the information flow, as in the credit example, is largely among parties whom the con-

sumer may not directly see; the cost of reaching consumers; and also the fact—and one that is often overlooked—that many uses of information are interrelated. So if we want information available for, say, fraud detection and crime detection, the way the cost of that is often borne is by other users who use that information for other purposes. If you eliminate those other purposes, you inevitably affect the availability of that information for those purposes.

I see my time is up, so I will stop.

[The prepared statement of Fred H. Cate follows:]

PREPARED STATEMENT OF FRED H. CATE, DIRECTOR, INFORMATION LAW AND COMMERCE INSTITUTE, INDIANA UNIVERSITY SCHOOL OF LAW

Mr. Chairman: My name is Fred Cate, and I am a professor of law and director of the Information Law and Commerce Institute at the Indiana University School of Law in Bloomington. For the past 12 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a visiting fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today and, more importantly, I want to acknowledge you and the Members of the Subcommittee for holding such a broad hearing on the subject of "Privacy in the Consumer World." It is a rare pleasure to participate in a hearing that is not restricted to a particular bill or event, but rather inquires widely about the uses of personal information, the need for further legislation, and the potential impact of adopting new privacy laws. Such an open-minded approach in an area as complex and important as privacy is desperately needed, and I applaud your leadership in providing it.

I would like to take advantage of the presence of the other distinguished members on this panel, who I believe will address a number of the issues posed by privacy laws, and limit my testimony to three points: the critical roles that information plays in our economy and society; the extent to which privacy laws inevitably interfere with the benefits that consumers enjoy as a result of accessible personal information; and the ways in which requiring consumer "consent" exacerbates, rather than ameliorates, the harmful impact of many privacy laws on consumers.

1. THE INFORMATION INFRASTRUCTURE

Information is the lifeblood of our 21st century economy. In the words of the Federal Reserve Board: "[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy." [1] These simple words reflect a profound transformation: Consumers are increasingly evaluated today according to more complete, objective, and reliable information about them than was ever before possible. As a result, consumers can now expect—and the law can meaningfully require—that they be treated as *individuals* and judged on their own records, not by their race, gender, who they know, or other subjective prejudices. This is the result of the information revolution: Routine, comprehensive information collection has contributed to unprecedented prosperity, and allows more Americans than ever before to share in that prosperity, and to do so on a more equitable basis. Consider the following examples of benefits that this "information infrastructure" makes possible.

a. Expanding the Availability, Enhancing the Speed, and Lowering the Cost of Consumer Credit

The routine sharing of reliable, standardized personal information has greatly expanded the availability, increased the speed, and reduced the cost of consumer credit. So, for example, when a consumer applies for a mortgage, car loan, or instant credit, the lender makes its decisions about whether, how much, and on what terms to lend based on information collected from a wide variety of sources over time. The lender can have confidence in that information because it has been assembled routinely—not just for the purpose of one loan application—and presents a complete picture of the borrower's financial situation—not just one moment in time or information from just a selective sample of the businesses with which the borrower

[1] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (1997).

deals. Because of that confidence, lenders provide more loans to a wider range of people than ever before. Between 1956 and 1998, the number of U.S. households with mortgage loans more than trebled. The same trend is true for credit card products; today, the average American adult carries 13 credit cards.

Consumers benefit by obtaining the funds they need to buy homes and cars and finance educations. The "almost universal reporting" of personal credit histories, in the words of economist Walter Kitchenman, is the "foundation" of consumer credit in the United States and a "secret ingredient of the U.S. economy's resilience."[2] In addition, because the necessary information does not have to be collected from scratch, loan applications are reviewed and approved faster than ever before. In 1997, 82% of automobile loan applicants received a decision within an hour; 48% of applicants received a decision within 30 minutes.[3] Many retailers open new charge accounts for customers at the point of sale in less than two minutes. This is unheard of in countries where restrictive laws prevent credit bureaus and other businesses from routinely collecting the information on consumer activities required to maintain the accurate, up-to-date files necessary to support rapid and accurate decision making.

The greater accuracy, speed, and efficiency of the credit system, and the greater confidence of lenders also drives down the cost of credit. Lenders don't have to charge higher interest rates and fees to guard against bad or missing information. And it is easier for lenders to pool loans according to risk and sell them in the secondary market—a process known as "securitization." This makes more capital available for new loans and further reduces the cost of credit in the United States by an estimated $80 *billion* per year for mortgages alone.[4] Most importantly, consumers benefit from the knowledge that loan decisions will now be based on their own financial situation, not on local biases or prejudices. Readily available, standardized personal information not only makes this possible, it also facilitates easy analysis of lender compliance with fair lending laws.

b. Identifying and Meeting Consumer Needs

Businesses use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences."[5] In short, information-sharing allows businesses to ascertain customer needs accurately and meet those needs rapidly and efficiently. Detailed consumer information is at the heart of new individualized offerings that provide each customer with the recognition and personalized service that she desires.

c. Enhancing Customer Convenience and Service

Information-sharing also enhances customer convenience and service. For example, many services are provided through a myriad of companies. A customer may have a checking account, a savings account, a credit card, and an investment account all with the same bank, but the four services will likely be provided by four completely separate affiliates. The customer's checks will be printed by a separate company altogether. Billing for the credit card may be handled by still another company. Because of information-sharing, the customer can deal with all six entities as if they were one. Her high savings balance may be used to qualify her for free checking. Overdrafts on her checking account can be covered automatically with her credit card. She can call one customer service number with questions, and if her credit card or checks are stolen, a single call is all that is needed to protect all of her accounts.

Many retailers provide specialty services and products, such as fine jewelry, photographic studios, vision services, hair care, and product repair or installation through independent companies that license the retailer's name, but are not the retailer's affiliates. This approach is required because of the nature of the service, efficiencies that come with specialization, insurance factors, and federal and state tax and licensure laws. Due to routine information-sharing, these independent companies provide services to customers under the retailer's name, accept the retailer's credit card, include information and coupons in the retailer's mailings and adver-

---

[2] Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns* 1 (The Tower Group 1999).

[3] Consumer Bankers Association, *1998 Automobile Finance Study* at 19.

[4] Kitchenman, supra, at 7.

[5] Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).

tisements, participate in the retailer's loyalty programs, and, from a customer perspective, are simply another department of the retailer's operations.

d. Targeting Interested Consumers

Information-sharing also allows consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested. As a result, information on second mortgages and home improvement services can be targeted only to home owners. Information on automotive products and services are targeted only to car owners. The American Association of Retired People can target its offers only to older Americans, veteran's organizations can appeal only to people who have served in the armed forces, and political campaigns can target their solicitations to registered members of their party.

In the absence of information-sharing, these organizations either (1) could not afford to communicate with potential customers or members, or (2) they must contact even more households—meaning more unsolicited mail, e-mail, and telephone calls—to find people interested in their offer. The first alternative would mean the death of many organizations. In fact, the cost of alerting consumers about a new product or opportunity can be a major obstacle to the launch of new businesses and prevent innovative products from ever reaching the marketplace. The second alternative means that the public is peppered with more mail, e-mail, and telephone calls, a higher percentage of which will be of no interest to the recipient. This would truly be "junk mail," because it would have been generated without regard for the recipient's demonstrated interests. Targeting marketing to consumer interests lowers the volume, cost, and environmental impact of that marketing while increasing consumer satisfaction.

e. Promoting Competition and Innovation

Information-sharing is especially critical for new and smaller businesses, which lack extensive customer lists of their own or the resources to engage in mass marketing to reach consumers likely to be interested in their products or services. This may help explain why some large European national banks and industrial concerns supported new privacy laws there: By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition from other countries or start-ups. Open access to third-party information and the responsible use of that information for targeted marketing is essential to level the playing field for new market entrants.

Similarly, businesses offering specialized products and services rely on accessible information to help them identify and reach those customers most likely to be interested in their offerings, wherever those customers are located. Many businesses in today's markets never see their customers because transactions are conducted exclusively by telephone, Internet, or mail. These businesses are able to serve the needs of potential customers they have never met because of the free flowing information that allows them to identify who those likely customers are. In a global market, information-sharing is key to connecting far-flung customers and businesses.

f. Preventing and Detecting Fraud

Another key use of personal information is to prevent and detect fraud. More than 1.2 million worthless checks are cashed at retailers, banks, and other U.S. businesses every day, accounting for more than $12 billion in annual losses.[6] Treasury Department officials estimated that credit card fraud losses would be between $2 billion and $3 billion in 2000.[7] The insurance industry paid $24 billion—10% of all claims—in 1999 for fraudulent property and casualty claims.[8] The GAO found that Medicare made improper payments of $13.5 billion in fiscal year 1999 alone, and has estimated that health care fraud accounts for up to 10% of national health care spending each year.[9] Across the economy, business losses due to all forms of document fraud and counterfeiting exceed $400 billion—6% of annual revenue of Amer-

---

[6] Barry Flynn, "In Search of Security, Some Banks Are Giving the Thumbs up to Fingerprinting New Customers," *Orlando Sentinel,* March 2000, at B1; Steven Marjanovic, "Banks Tap ATM Systems To Banish 18B Checks," *American Banker,* June 14, 2000, at 1.

[7] Gary Fields, "Victims of Identity Theft Often Unaware They've Been Stung," *USA Today,* March 15, 2000, at 6A (quoting Undersecretary James Johnson of the U.S. Treasury Department).

[8] "Insurance Fraud," *III Insurance Issues Update,* Oct. 2000.

[9] General Accounting Office, *Medicare Improper Payments: While Enhancements Hold Promise for Measuring Potential Fraud and Abuse, Challenges Remain* (GAO/AIMD/OSI-00-281) at 4 (2000).

ican businesses—per year.[10] Although businesses paid for virtually all of these losses, they ultimately affect consumers through higher prices, inconvenience, and lost time and productivity.

Personal information is one of the most effective tools for stemming these losses. Such information is used every day to identify consumers cashing checks and seeking access to accounts. Close monitoring of account activity also allows credit providers, insurance companies, and other businesses to recognize unusual behavior that may indicate that someone is using a credit card or debit card without authorization or making improper claims. Moreover, because of information-sharing, companies share alerts about lost or stolen credit or debit cards and information about fraud schemes so that they can prevent further losses and improve the odds of apprehending the thief.

g. Informing the Electorate and Protecting the Public

Personal information is also used for a wide variety of purposes central to democratic self-governance and protecting public health and safety. For example, information is used to elect and monitor public officials and to facilitate public oversight of government employees and contractors. The Supreme Court has found that these uses are so critical that it has virtually eliminated any recourse by public officials or public figures for the publication of true information, even if defamatory or highly personal.[11]

Law enforcement officials rely on collected personal information to prevent, detect, and solve crimes. Journalists and other researchers use accessible information to inform the public about matters of public importance. Personal information is also used for product safety warnings and recall notices, such as when Firestone and Ford Motor Company used databases to identify and obtain current addresses for people who own recalled Firestone tires.

Medical researchers rely heavily on personal information to conduct "chart reviews" and perform other research that is critical to evaluating medical treatments, detecting harmful drug interactions, uncovering dangerous side effects of medical treatments and products, and developing new therapies. Such research *cannot* be undertaken with wholly anonymous information, because the detailed data that researchers require will always include information that *could* be used to identify a specific person, and when that information indicates that a given therapy or drug poses a real health risk, researchers *must* notify the affected individuals.

Even information as mundane as citizen addresses is used to locate missing family members, owners of lost or stolen property, organ and tissue donors, and members of associations and religious groups and graduates of schools and colleges; and to identify and locate suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. (This same information is used to help verify the identity of consumers who apply for instant credit, begin new utility service, or seek other valuable products and services.)

These examples are not exhaustive; they are mere illustrations of the extent to which personal information constitutes part of this nation's essential infrastructure, the benefits of which are so numerous and diverse that they impact virtually every facet of American life.

2. THE PRIVACY TENSION

All of the benefits outlined above flow from readily accessible information about consumers. To provide those and other benefits, access to data is essential. Laws and regulations designed to protect privacy interfere with that access and therefore with the benefits that result from open information flows. As a result, those laws—although motivated by the best of intentions—inevitably harm consumers. In the words of one state Attorney General, because privacy laws interfere with information flows, consumers ultimately pay the price for those laws "in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."[12] But the harm to consumers is also experienced through reduced convenience and service, an increased number of less well-targeted commercial solicitations, limited competition and innovation, and even diminished public health and safety.

---

[10] Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse* <http://www.cfenet.com/newsandfacts/fraudfacts/reporttothenation/reportsection4.shtml>.

[11] Monitor Patriot Co. v. Roy, 401 U.S. 265 (1971).

[12] Bill Pryor (R-Ala.), *Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium,* July 11, 2000, Washington, DC, at 4.

3. THE LIMITS OF CONSENT

Proponents of new privacy laws often argue that these costs can be avoided because most privacy laws do not block information flows outright, but rather condition them on consumer *consent.* This reflects the recent dominant trend in privacy legislation—to invest consumers with near absolute *control over information,* what Alan Westin, in his path-breaking study *Privacy and Freedom,* described as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [13] The National Association of Attorneys General's December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: "Put simply, consumers should have the right to know and *control* what data is being collected about them and how it is being used, whether it is offline or online." [14] And virtually all of the privacy bills pending before Congress reflect this goal: "To strengthen *control* by consumers" and "to provide greater individual control." [15]

As a result, proponents of privacy laws argue that the costs of these laws can be avoided, because if consumers are persuaded that they benefit from information flows, they will consent to the collection and use of information about them. The simple, straightforward nature of this argument has made it very powerful. However, in addition to conflicting with Supreme Court precedent on the ownership of information [16] and the protection of expression, [17] this approach ignores the practical difficulty and burden to consumers of attempting to exercise control over the vast amount of data that they generate and disclose about themselves in a increasingly networked economy, and ignores the many powerful reasons why society permits access to information about others.

a. Unanticipated Benefits

The benefits of personal information are often unanticipated. For example, many retailers collect information about consumer purchases and then access that information so that consumers can return merchandise without a receipt, order supplies and replacement parts without knowing the exact model number or specific product information, obtain information about past purchases for insurance claims when fire or other disasters destroy or damage those goods, and receive immediate notification about product recalls and other safety issues. These are tangible benefits that many consumers take advantage of every day, but few consumers would anticipate in advance that they were going to need information about a past transaction for insurance purposes or to order replacement parts. The benefit is exceptionally valuable when it is needed, but often illusory before that time.

b. Lack of Consumer Contact

Many benefits result from uses of personal information that do not involve the consumer directly. For example, credit bureaus update consumer credit files—the files that are used to obtain rapid, low cost access to credit of all forms—without ever dealing directly with the consumer. In fact, few Americans will ever deal directly with a credit bureau. To require the credit bureau to establish contact with the consumer every time it needed to collect or use information about him or her would be expensive and burdensome to the consumer. Similarly, most mailing lists are obtained from third parties, not the people whose names are on the list. For a secondary user to have to contact every person individually to obtain consent to use the information would cause delay, require additional contacts with consumers, and increase costs.

c. Value of Standardized and Third-Party Information

There are many beneficial uses of personal information where the benefit, frankly, is derived from the fact that the consumer has *not* had control over the information. This is certainly true of credit information: Much of its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make not only that credit report useless, but all others, because lenders, merchants, employers, and others who rely on credit reports would not know which ones con-

---

[13] Alan F. Westin, *Privacy and Freedom* 7 (1967).

[14] National Association of Attorneys General, *Draft Statement on Privacy Principles and Background* at 7 (Dec. 11, 2000) (emphasis added).

[15] S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong. § 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001) (emphasis added)

[16] See, e.g., United States v. Miller, 425 U.S. 435 (1976).

[17] See, e.g., Martin v. Struthers, 319 U.S. 141 (1943); Lamont v. Postmaster General, 381 U.S. 301 (1965); Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Comm'n, 518 U.S. 727 (1996).

tained only selective information. Even when information is not particularly "positive" or "negative," its value may depend on it being complete. Many businesses monitor accounts for suspicious activity that may indicate fraudulent activity. Often credit card companies will call a card holder whose account has experienced unusual charges to verify that the card has not been stolen. Identifying the *unusual* requires knowing what is *usual* and that, in turn, requires access to a complete set of data.

d. Consumer Preferences

Most consumers do not want to be deluged with repeated requests for consent. The ultimate result is that consumers will either not consent, and thereby diminish the benefits that flow from information-sharing both for themselves and others, or they will consent to everything, just to avoid further calls, letters, and e-mails. The *Los Angeles Times* reported in December 1999 that banking customers are understandably "irritated if the bank fails to inform them that they could save money by switching to a different type of checking account." As the newspaper noted, however, "to reach such a conclusion, the bank must analyze the customer's transactions."[18] One major U.S. bank reported that its customers who participated in a test of various privacy policies were annoyed at the very idea of being contacted by the bank to obtain permission to contact them again in the future to offer selected opportunities. Customers expected that the bank would use their information to offer them appropriate offers. The last thing they wanted was another phone call or letter asking permission to do what they perceived to be the very foundation of their relationship with the institution.

e. The Practical Obstacles to Consumer Contact

Conditioning use of personal information on specific consent may also harm consumers because of the practical difficulties of reaching them. Consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. To obtain permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls, and one-third of their customers were denied opportunities to receive information about valuable new products and services.[19]

f. The Cost of Obtaining Consent

There is always a price to obtaining consent and recent experience has shown that those costs are often quite significant. For example, the privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act require financial institutions to "clearly and conspicuously" provide customers with a notice about its policies and practices for disclosing personal information and informing customers about their right to "opt-out" of certain sharing of that information.[20] That disclosure must be made "[a]t the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship."[21] By July 1, 2001, approximately 40,000 financial institutions will be sending as many as 2-5 billion notices to their various customers. Households will receive an average of 20 or more notices each. Printing and mailing costs alone will run into the *billions* of dollars. Internal compliance costs are certain to be much higher.

"Opt-in" systems cost even more. The Department of Health and Human Services calculates that compliance with its recently released Health Insurance Portability and Accountability Act privacy rules will cost $3.2 billion for the first year, and $17.6 billion for the first ten years.[22] Based on the prior, less complicated draft of the rules, health care consulting companies have calculated that the cost will be much higher—between $25 and $43 billion (or three to five times more than the industry spent on Y2K) for the first five years for compliance alone, not including impact on medical research and care or liability payments.

These costs are inevitably passed on to consumers. If the market will not bear the added cost, then these costs mean that the service or product will not be offered.

---

[18] Edmund Sanders, "Your Bank Wants to Know You," *Los Angeles Times,* Dec. 23, 1999, at A1.

[19] Brief for Petitioner and Interveners at 15-16, U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

[20] Gramm-Leach-Bliley Financial Services Modernization Act tit.V, 106 Pub. L. No. 102, 113 Stat. 1338 (1999) (codified at various sections of 15 U.S.C.).

[21] 15 U.S.C. § 503(a).

[22] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

g. The Interconnectedness of Consent

Many of the beneficial uses of information that consumers now enjoy depend on spreading the cost of collecting and maintaining the information for a variety of uses. For example, commercial intermediaries collect, organize, and make accessible to the public government records. Those records are used for countless socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from "deadbeat" parents and spouses, and many others. In fact, in 1998 the FBI alone made more than 53,000 inquiries to commercial online databases for "public record information" that led to the arrest of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.[23] The Association for Children for Enforcement of Support uses information from public records, provided through commercial vendors, to locate over 75% of the parents they sought.[24] Access to these records is possible, as well as convenient and inexpensive, precisely because commercial intermediaries assemble the information for such a wide variety of other uses. If the law restricted the other valuable uses of public records, or made those uses prohibitively expensive, then the data and systems to access them would not be in place for *any* use. In as much as the beneficial uses of information outlined above are interconnected, and often depend on common systems and spreading the cost of acquiring and managing data over many uses, consent-based laws may only create the *illusion* of consent, because they will lead to consumers having fewer opportunities made available to them to which they *can* consent.

h. Required Consent

The opportunity for consent may also be illusory because many services or products cannot or will not be provided without personal information. HIPAA, for example, requires that physicians provide extensive disclosures and obtain explicit consent concerning information collection and use prior to treating a patient. If a patient wishes to be treated, she must consent. The law is effectively irrelevant, because the physician cannot treat the patient without information about his or her condition. Moreover, as a practical matter, signing the consent form is likely to become just another procedural hurdle, like signing an insurance authorization form, to getting in to see a doctor. Experience suggests that few people will shop for physicians based on information policies; rather, their decisions about from whom to seek service will be driven by price, location, insurance coverage, specialty, and other considerations. So the expense of crafting, providing, and storing consent forms will likely achieve little in terms of enhancing consumer choice or privacy.

i. Consumer Ignorance and Lethargy

Finally, even if the request gets through to the intended adult recipient, the typical response to requests for consent to use personal information, to judge by the extensive experience of businesses and not-for-profit organizations, is that the customers will simply ignore them. Most unsolicited mail in this country is discarded without ever being read and most unsolicited commercial or fund-raising telephone calls are terminated by the consumer without the offer ever being made. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Even where mail is actually read and the offer appeals to the consumer, lethargy and the competing demands of busy lives usually conspire to ensure that no action is taken. It is difficult to imagine that promises of potential future benefits from information use will command greater attention or activity.

These considerations suggest that simply conditioning the use of personal information on specific consent is tantamount to prohibiting outright many beneficial uses of information, because of the cost of obtaining consent, the extent to which consent may undermine information's usefulness, the degree to which uses of information are interconnected, and the many impediments to consumers receiving and acting on the request, even when it is in their best interest to do so.

---

[23] Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Senate Comm. on Appropriations, March 24, 1999 (statement of Louis J. Freeh).

[24] Hearings before the House Committee on Banking and Financial Services, July 28, 1998 (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).

CONCLUSION

The fact that information flows constitute a central part of our economic and social infrastructure, and that privacy laws—by interfering with those information flows—inevitably harm consumers and businesses, does not suggest that there is no role for the government or for law in protecting privacy. Far from it.

The government plays many critical roles in helping to protect individual privacy. One of the most important responsibilities of the government is assuring that its own house is in order. Only the government has the power to compel disclosure of personal information and only the government operates free from market competition and consumer preferences. As a result, the government has special obligations to ensure that it complies with the laws applicable to it; collects no more information than necessary from and about its citizens; employs consistent, prominent information policies through public agencies; and protects against unauthorized access to citizens' personal information by government employees and contractors.

Similarly, there are many steps that only the government can take to protect citizens against privacy-related harms, such as identity theft: Make government-issued forms for identification harder to obtain; make the promise of centralized reporting of identity thefts a reality; make it easier to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief. The government alone has this power.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so.

The government should also help educate the public about privacy and the tools available to every citizen to protect her own privacy. Many privacy protections can only be used by individuals—no one else can protect their privacy for them. Yet few individuals will recognize the importance of their responsibility or have the knowledge to fulfill it without education.

Finally, should you conclude that new laws or regulations are necessary, it is critical to identify and articulate clearly the purpose of the proposed privacy law or regulation, and whether it will in fact serve that purpose: In sum, what public benefit justifies the government's action? Only after having answered this question can the benefits of the proposed law or regulation be balanced against both the beneficial uses of information with which it interferes and the other costs of implementing and complying with the law. Armed with this information, you can then ask whether the law is worth its cost or whether there are other less intrusive, less expensive, or more effective tools for achieving the same purpose.

I address these and related issues in greater detail in a report that will forthcoming soon from the American Enterprise Institute. Because that document is so directly responsive to the subject of this hearing, with your permission, I append the complete draft report to my testimony.

Thank you again for the opportunity to testify.

Mr. STEARNS. Thank you.

Professor Volokh?

STATEMENT OF EUGENE VOLOKH

Mr. VOLOKH. Thank you. Mr. Chairman, members of the subcommittee, it is a great pleasure and honor to be invited to testify here. I will limit my remarks to the First Amendment questions posed by certain kind of privacy rules and will not speak to whether they are a good policy or bad policy but solely to the Constitutional questions.

Why are there First Amendment problems involved here? I mean, isn't privacy sort of one of those wonderful, warm, fuzzy things that sort of everybody should be in favor of? Well, the right to control information about ourselves sounds very appealing until you realize that what it means, literally what it means is the right to stop others from speaking about us, the right to stop others from communicating about us.

So let's look at what would happen if the right were taken to its logical conclusion, just read by its terms. If people had the right to control information about themselves, that means they could per-

haps sue us if we gossip about them to our friends. They could sue newspapers, as some people have tried to do, if they publish information that for whatever reason the subject of the information doesn't like—accurate information, but still, it's information about them. If the subject has the right to control information about himself, he should be able to stop newspapers from reporting it or stop his business partners, people who have done business with him, discussing the outcome and the terms of that transaction.

The right to control information about ourselves is the right to stop others from communicating this information, and whenever you start talking about rights to stop others from communicating, you run up against the First Amendment. In fact, people have talked about codes of fair information practices, and I would like to suggest that at least as to many kinds of practices, the First Amendment is our code of fair information practices, just as if you wanted to talk about a code of fair journalism practices or a code of fair political debate practices. You know, we're all in favor of fair journalism, of fair political debate, of fair information management. But in the case of fair journalism practices, of fair political debate practices, I would take it we would say it is not up to the Government to set up this code; this code already exists, and it is the First Amendment.

It seems to me that the same is, in large measure, true about other kinds of communication of information. Just to give a couple of very brief examples of where this tension comes up, there is a case from California where California courts recognized the so-called disclosure tort, which really does give people control of information about themselves. There is a Reader's Digest article that was published about somebody who was an armed robber. Ten years before, he had engaged in armed robbery involving a gun battle with the police, but the courts allowed him to sue when Reader's Digest reported this fact in kind of a story saying, you know, here is a story from the past about this formerly notorious crime.

The theory was, well, he has a right to privacy. And the court said, well, right-thinking people shouldn't want to know this information, and it used the term right-thinking people. And I submit that under the First Amendment, it is up to each of us to decide, using our own thinking, whether we want to know certain information and whether we want to communicate certain information that we have acquired, whether as a result of reading public records; a result of doing business with somebody; or as a result of talking to people about this person.

Now, it seems to me, as I said, that similar things arise in the context of many—not all—some of the proposals that I think might be quite sound, but many cyberspace information privacy speech restrictions are, indeed, speech restrictions.

Let me briefly make, I think, one distinction that I think is very important in this context, and that is between restrictions that merely enforce contracts, either expressed or implied contracts, and distinctions that go beyond that; that we do not have and should not have a right to control people from speaking about us, but we should have a right to insist that they keep their promises to us. So if somebody on their Website says I promise to keep your information private, it is certainly quite legitimate for the government,

either through a normal contract lawsuit or through, perhaps, FTC action and such, to enforce that. It seems to me, again, there might be policy questions as to what the best way of doing it is, but it would be quite Constitutional.

In certain situations, I think it is also legitimate for the government to say that we will infer a term, a privacy term, into the contract. I think that is how we can best understand things like attorney-client privilege and a variety of other such things; that when you go to an attorney, implicitly, the attorney is promising to keep certain information secret. And I think the government can establish these defaults in certain situations so long as the defaults are waiveable; so long as the person can say or the Website can say I stand on my rights as a speaker to communicate this information.

And I warn you up front: you know about it. If you deal with me, you have to understand that I am going to feel free to communicate information about you.

So if it is a truly contractual thing, including default terms, including more aggressive enforcement, then, it seems to me that would be a Constitutional thing. But if it goes beyond it, if it says we will impose this speech restriction, even in the noble name of privacy, we will impose this speech restriction on you even without any contractual understanding, that, it seems to me, poses very serious First Amendment problems.

My time is up, but I would be happy to discuss some of the doctrinal issues having to do with things like intellectual property arguments, which I think are unsound; commercial speech arguments, which I think don't apply here; and other First Amendment doctrines that I think ultimately support rather than contradict my conclusions.

[The prepared statement of Eugene Volokh follows:]

PREPARED STATEMENT OF EUGENE VOLOKH,[1] PROFESSOR OF LAW, UCLA LAW SCHOOL

INTRODUCTION

Privacy is a popular word, and government attempts to "protect our privacy" are easy to endorse. Government attempts to let us "control . . . information about ourselves"[2] sound equally good: Who wouldn't want extra control? And what fair-minded person could oppose requirements of "fair information practices"?[3]

The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits[4]), whether the communication

[1] Professor of Law, UCLA Law School (volokh@law.ucla.edu). This testimony is largely based on an article with the same title in 52 Stanford Law Review 1049 (2000), Copyright 2000 by Eugene Volokh and the Board of Trustees of the Leland Stanford Junior University.

[2] *See, e.g.,* Charles Fried, *Privacy,* 77 YALE L.J. 475 (1968); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet,* 34 SAN DIEGO L. REV. 1153, 1155 (1997).

[3] *See, e.g.,* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector,* 80 IOWA L. REV. 497 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States,* 80 IOWA L. REV. 553 (1995).

[4] *Cf., e.g.,* New York Times v. Sullivan, 376 U.S. 254, 265 (1964) (holding that the First Amendment applies to "civil lawsuit[s] between private parties," because such lawsuits involve "[state] courts . . . appl[ying] a state rule of law").

is "fair" or not.[5] While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.

Consider, for instance, the "disclosure of private facts" tort, which bars the media from reporting supposedly "nonnewsworthy" personal information that most people would find highly private.[6] On the one hand, it sounds appealing; by definition, if the information is "nonnewsworthy" and "private," why should anyone print it?

But under our free speech regime, should a government agency (such as a court) really be able to decide what is "newsworthy" or "of legitimate public concern"? Should, for instance, courts be able to hold—as California courts did—that the media may be punished for reporting that a college student politician is a transsexual, or that a person had committed armed robbery and engaged in a shoot-out with police ten years before?

True, some citizens might think that such reporting, in the words of one court, has no "public purpose" and was not "of legitimate public interest," that there was no "reason whatsoever" for it, and that "we, as right-thinking members of society, should permit [a person] to continue in the path of rectitude rather than throw him back into a life of shame or crime" by revealing his past.[7] Others, though, may disagree. And under the First Amendment, it should be up to each of us, as readers and publishers, to decide what we think is "of legitimate public interest," and not to have the government make the decision for us, even in the name of "privacy." The Supreme Court has never fully considered the constitutionality of the disclosure tort, but many courts have recognized the serious First Amendment problems that the tort poses.

Consider also *Bartnicki v. Vopper,* a currently pending Supreme Court case. In *Bartnicki,* an unknown person tape-recorded a cellular phone conversation in which two union officials were discussing the possibility of "blow[ing] off the[] front porches" of management. The tape eventually made its way to a radio station, which played it on the air. The station was then sued under a federal statute banning the media from publishing or even paraphrasing intercepted cellular phone conversations, even when the media entity was entirely innocent of the actual interception.[8]

Again, the law serves noble purposes: it seeks to protect people's privacy, and to deter illegal interception of cellular conversations (and everyone agrees that the interception itself should be illegal). But it does this by restricting the press's freedom to publish—the right to control information, we again see, is a right to stop others from speaking.

And the logic of the law of course doesn't stop at the rather unusual context of intercepted cell phone conversation: The same sort of law could easily be enacted to ban the publication of any material that's illegally *leaked* (for instance, in violation of an employer's nondisclosure agreement or a fiduciary duty of loyalty) as well as to the publication of material that's illegally *gathered.* The understandable desire to protect people's privacy can thus dramatically interfere with the media's freedom to report the news, and to the public's access to the news.

The same First Amendment objections apply, I will argue, to many recent proposals for laws securing information privacy on the Internet. Some people have argued that these proposals are different from the examples I give above, because they fall into some exceptions to First Amendment protection. And I agree that some such proposals, if they are framed as default contractual rules (such as true "opt-in" or "opt-out" provisions), or as disclosure requirements, are constitutional.

But other proposals are not constitutional, and the defenses which are most often given for them—the intellectual property argument, the commercial speech argument, the private concern argument, and the compelling government interest argument—are not sound under current First Amendment doctrine. And while one can urge courts to narrow current First Amendment law to accommodate these new proposals, I think that would be a serious mistake. If free speech principles are diluted in the attractive case of information privacy speech restrictions, such a decision will be a powerful precedent for still more restraints that might be proposed in the future.

Such slippery slope concerns are still quite sensible, because accepting a proposed speech restriction entails accepting a principle that is broader than the particular

---

[5] If "fair information practices" applied only to the government's control of its own speech, I would have had no objection to them. But governmental restriction of supposedly "unfair" speech by nongovernmental entities raises serious First Amendment problems.

[6] *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[7] Briscoe v. Reader's Digest Ass'n, 483 P.2d 34, 36, 41 (Cal. 1971).

[8] Bartnicki v. Vopper, 200 F.3d 109 (3rd Cir. 1999).

proposal and that can logically cover many other kinds of restraints.[9] Our legal system is based on precedent. Our political life is in large measure influenced by arguments by analogy. And many people's normative views of free speech are affected by what courts say: If the legal system accepts the propriety of laws mandating "fair information practices," people may becomes more sympathetic to legal mandates of, for instance, fair news reporting practices or fair political debate practices.[10]

I ultimately conclude that these risks of watering down important free speech protections are troubling enough that I must reluctantly oppose such information privacy rules. But I hope my views will also be useful to those who are committed to supporting information privacy speech restrictions, but would like to design their arguments in a way that will minimize the risks that I identify.

Thinking ahead about the possible unintended implications of a proposal—even, and perhaps especially, if it seems viscerally appealing—is always worthwhile.

I. INFORMATION PRIVACY SPEECH RESTRICTIONS

My analysis focuses on the government acting as sovereign, restricting what information nongovernmental speakers may communicate about people. I thus exclude restrictions that the government imposes on its own agencies, such as Freedom of Information Act provisions that prevent government revelation of certain data, or IRS or census rules that prohibit the communication of some tax or census data to other government agencies or to the public. By focusing on communication by nongovernmental speakers—reporters, businesspeople, private detectives, neighbors—I limit the inquiry to people and organizations that indubitably have free speech rights.

I also exclude restrictions that the government imposes as an employer (e.g., telling its employees that they may not reveal confidential information learned in the course of employment), or as a contractor putting conditions on the communication of information that it has no constitutional duty to reveal (e.g., telling people who want certain lists from the Federal Election Commission that they may only get them if they promise not to use those lists for certain purposes, or telling litigants that they will get discovery materials only if they promise not to reveal them). The

---

[9] One of the most eloquent American expressions of this concern with uncabinable principles is also among the earliest:

[I]t is proper to take alarm at the first experiment on our liberties. We hold this prudent jealousy to be the first duty of citizens, and one of [the] noblest characteristics of the late Revolution. The freemen of America did not wait till usurped power had strengthened itself by exercise, and entangled the question in precedents. They saw all the consequences in the principle, and they avoided the consequences by denying the principle. We revere this lesson too much, soon to forget it. Who does not see that the same authority which can establish Christianity, in exclusion of all other Religions, may establish with the same ease any particular sect of Christians, in exclusion of all other Sects? That the same authority which can force a citizen to contribute three pence only of his property for the support of any one establishment, may force him to conform to any other establishment in all cases whatsoever?

James Madison, *Remonstrance Against Religious Assessments* (1786). I likewise fear that the same authority which can force a citizen to stop speaking on one matter by, for instance, defining it out of the zone of "legitimate public concern" may in time do the same as to speech on other matters.

[10] For some examples of past attempts to restrict such "unfair" speech, see, e.g., Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (rejecting attempt to impose liability for a publisher's vicious parody of a political enemy); Miami Herald v. Tornillo, 418 U.S. 241 (1974) (rejecting attempt to require a newspaper to publish rebuttals of attacks on a consolidate); Keefe v. Organization for a Better Austin, 402 U.S. 415 (1971) (rejecting attempt to enjoin leafletting aimed at pressuring a local resident to change his business practices); Mills v. Alabama, 384 U.S. 214 (1966) (rejecting attempt to ban election-day political editorials in the interests of preventing unrebuttable attacks).

The European Personal Data Directive, which is often praised by privacy advocates, does require countries to create a code of fair news reporting practices: It on its face applies to journalism that reveals personal data such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," and mandates that governments create exemptions for journalism, art, or literature "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." Directive 95/46/EC, 1995 O.J. (L 281) 31, arts. 8(1), 9. What this provision will ultimately mean is so far unclear. *Cf.* James R. Maxeiner, *Freedom of Information and the EU Data Protection Directive,* 48 FED. COMM. L.J. 93, 102 (1995) (stating that the "only if they are necessary" language was added to prevent "the balance [from] fall[ing] too much in favor of the media," and concluding that the scope of the journalism exception is uncertain); Paul Eastham, *I Would Have Gagged the Press Over Cook,* LONDON DAILY MAIL, Feb. 5, 1998, at 2 (quoting the senior English Law Lord as taking the view that the privacy directive would have barred certain news stories about a cabinet minister's alleged affair).

The disclosure tort, of course, has always been an attempt to mandate fair news reporting practices.

government has long been held to have much broader powers when it's acting as employer or contractor, imposing constraints on those who assume them in exchange for government benefits or for access to government records, than when it's acting as sovereign, controlling the speech of private citizens.

I also focus only on restrictions on communication. Other things that are often called privacy rules—the right to be free from unreasonable governmental searches and seizures, the right to make certain decisions about one's life without government interference, the right not to have people listen to you or watch you by going onto your property, the right not to have people electronically eavesdrop on your conversations, the requirement that credit bureaus notify consumers when credit reports about them are prepared, and the like—are outside the scope of my discussion.

Some of these laws, for instance restraints on government snooping or control, pose no First Amendment problems. For other laws, such as restrictions on nongovernmental gathering of information through nonspeech means, the First Amendment rules are unclear; but it is clear that the analysis of restrictions on information gathering is different from the analysis of restrictions on speech. It is the latter doctrine that is most fully developed, and that provides the most protection against government restrictions.

These three exclusions merely reflect the fact that the strongest protection of free speech has long been seen as arising when the government is acting as sovereign, restricting the speech of private parties. And within this zone lie a variety of current and proposed speech restrictions, including both older rules such as the disclosure tort, and newer ones such as some proposed restrictions on businesses revealing information about their customers.

II. CONTRACT

A. Permissible Scope

To begin with, one sort of limited information privacy law—contract law applied to promises not to reveal information—is eminently defensible under existing free speech doctrine. The Supreme Court explicitly held in *Cohen v. Cowles Media* that contracts not to speak are enforceable with no First Amendment problems.[11] Enforcing people's own bargains, the Court concluded (I think correctly), doesn't violate those people's rights, even if they change their minds after the bargain is struck. Insisting that people honor their bargains is a constitutionally permissible "code of fair practices," whether information practices or otherwise.

And such protection ought not be limited to express contracts, but should also cover implied contracts (though, as will be discussed below, there are limits to this theory). In many contexts, people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract—that part of what their contracting partner is promising is confidentiality.

Furthermore, though *Cohen v. Cowles Media* involved traditional enforcement of a promise through a civil suit, there should be no constitutional problem with the government enforcing such promises through administrative actions, or using special laws imposing presumed or even punitive damages for breaches of such promises.

I suspect that even with purely contractual remedies, the threat of class action suits could be a powerful deterrent to breaches of information privacy contracts by e-commerce sites, especially since the suits would create a scandal: In the highly competitive Internet world, a company could lose millions in business if people hear that it's breaking its confidentiality promises. But I think it would be constitutional for the government to try to increase contractual compliance either by providing an extra incentive for aggrieved parties to sue or by bringing a complaint itself.

The great free speech advantage of the contract model is that it does not endorse any right to "stop people from speaking about me." Rather, it endorses a right to "stop people from violating their promises to me." One such promise may be a promise not to say things, and perhaps there may even be special defaults related to such promises or special remedies for breaches of such promises.

The government may enforce obligations that the would-be speaker has himself assumed. And such enforcement, in my view, poses little risk of setting a broad precedent for many further restrictions, precisely because it is founded only on the consent of the would-be speaker, and thus cannot justify the other speech restraints to which the speaker has not consented.

---

[11] 501 U.S. 663 (1991).

B. Limitations

Contract law protection, though, is distinctly limited, in two ways.

First, it only lets people restrict speech by parties with whom they have a speech-restricting contract, express or implied. If I make a deal with a newspaper reporter under which he promises not to identify me as a source, I can enforce the deal against the reporter and the reporter's employer, whom the reporter can bind as an agent. But if a reporter at another news outlet learns this information, then that outlet can publish it without fear of a breach of contract lawsuit.

Second, *Cohen v. Cowles Media* cannot validate speech-restrictive terms that the government compels a party to include in a contract; the case at most validates government-specified defaults that apply unless the offeror makes clear that these terms aren't part of the offered deal. Thus, while the government may say "Cyberspace sales contracts shall carry an implied warranty that the seller promises not to reveal the buyer's personal information," it may not add "and this implicit warranty may not be waived, even by a prominent statement that is explicitly agreed to by a customer clicking on an 'I understand, and agree to the contract in spite of this' button."

This flows directly from the rationale on which *Cohen v. Cowles Media* rests: "The parties themselves . . . determine the scope of their legal obligations, and any restrictions which may be placed on the publication of truthful information are self-imposed." A merchant's express promise of confidentiality is "self-imposed"; so, one can say, is an implicit promise, when the merchant had the opportunity to say "by the way, I am not waiving my rights to speak about this transaction and am thus not promising confidentiality" but didn't do so. But when someone is legally barred from communicating, even if he explicitly told his contracting partner that he was making no such promise, then such an obligation is hardly "self-imposed" or determined by mutual agreement.

Thus, I certainly do not claim that a contractual approach to information privacy, even with a large dollop of implied contract, is a panacea for information privacy advocates. There is much that information privacy advocates may want but that contract will not provide. I claim only that contractual solutions are a constitutional alternative and may be the only constitutional alternative, not that they are always a particularly satisfactory alternative.

C. Contracts with Children

Finally, this discussion of contracts presupposes that both parties are legally capable of entering into the contract and of accepting a disclaimer of any implied warranty of confidentiality. If a cyber-consumer is a child, then such an acceptance might not be valid. This is also a difficult issue, but one that is outside the scope of this Article.[12]

III. PROPERTY

A. Intellectual Property Rules as Speech Restrictions

Partly because of the limitations of the contract theory, many information privacy advocates argue that people should be assigned a property right in personal information about themselves.[13] Such a property approach would bind everyone, and not just those who are in contractual privity with the person being talked about.

Database operators would have to stop communicating information about people unless people give permission, even though the database operators have never promised, expressly or implicitly, to keep silent. Likewise, people could stop newspapers from publishing stories about them, even if the information was gleaned through interviews with third parties or was taken (with no contractual constraints) from public records.[14]

Calling a speech restriction a "property right," though, doesn't make it any less a speech restriction, and it doesn't make it constitutionally permissible. Broad, pre-*New York Times v. Sullivan* libel laws can be characterized as protecting a property

---

[12] *Cf.* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 *et seq.*; Justin Matlick, *Governing Internet Privacy: A Free-Market Primer* (Pacific Research Institute, July 1999), (visited March 3, 2000) <http://www.pacificresearch.org>; Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector,* Cato Policy Analysis No. 295 (Jan. 22, 1998) <http://www.cato.org/pubs/pas/pa-295.html>, text accompanying nn.76-79.

[13] *See, e.g.,* Lawrence Lessig, *The Architecture of Privacy,* VAND. J. ENT. L. & PRAC., April 1999, at 56, 63.

[14] *See* Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory,* 12 GA. L. REV. 429, 439-40 (1978).

right in reputation; in fact, some states consider reputation a property interest.[15] The right to be free from interference with business relations, including interference by speech urging a boycott as in *NAACP v. Claiborne Hardware,*[16] is often seen as a property right.[17]

Restrictions on speech that uses cultural symbols in ways that the cultures find offensive might likewise be reframed as property rights in those symbols.[18] A ban on all unauthorized biographies, whether of former child prodigies, movie stars, or politicians, can be seen as securing a property interest in the details of those people's lives. Similarly, an early right of publicity case took the view that people who aren't public figures have the exclusive right to block all photos and portraits of themselves, with no exceptions for news stories.[19]

Each of these "property rights," though, would remain a speech restriction. A property right is, among other things, the right to exclude others;[20] an intellectual property right in information is the right to exclude others from communicating the information—a right to stop others from speaking. Like libel law, intellectual property law is enforced almost entirely through private litigation, but like libel law, it's still a government-imposed restriction on speech.[21] Some such restrictions may be permissible because there's some substantive reason why it's proper for the government to restrict such speech, but not *because* they are intellectual property rights.

The question isn't (as some suggest) "who should own the property right to personal information?"[22] Rather, it's whether personal information should be treated as property at all—whether some "owner" should be able to block others from communicating this information, or whether everyone should be free to speak about it.

B. Existing Restrictions as Supposed Precedents

The Court has, of course, upheld some intellectual property rights against First Amendment challenge, acknowledging that they are speech restrictions but holding that those restrictions were constitutional. In all these precedents, though, the Court has stressed a key point: The restrictions did not give the intellectual property owners the power to suppress facts. And this power to suppress facts is exactly the power that information privacy speech restrictions would grant.[23]

Harper & Row v. Nation Enterprises, which held that copyright law is constitutional,[24] is the best example of this. Under copyright law, I may not publish a book that includes more than a modicum of creative expression from your book, even though my book is neither obscene nor libelous nor commercial advertising; such a restriction, *Harper & Row* held, is indeed a speech restriction, but a permissible one.

But the main reason *Harper & Row* gave for this conclusion is that copyright law does not give anyone a right to restrict others from communicating facts or ideas. "[C]opyright's idea/expression dichotomy strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting *free communication of* facts while still protecting an author's expression." "No author may copyright his ideas or *the facts he narrates.*"

Copiers "possess[] an unfettered right to use *any factual information* revealed in [the original]," though they may not copy creative expression. There ought not be "abuse of the copyright owner's monopoly as an instrument to suppress *facts*." "In

---

[15] Reputation is generally not a property interest for purposes of the federal Due Process Clause, Paul v. Davis, 424 U.S. 693 (1976), but it can be a property right for other purposes. *E.g.,* Marrero v. City of Hialeah, 625 F.2d 499, 514 (5th Cir. 1980).

[16] 458 U.S. 886 (1982).

[17] *E.g.,* Leonard Duckworth, Inc. v. Michael L. Field & Co., 516 F.2d 952, 955 (5th Cir. 1975).

[18] *Cf.* Hornell Brewing Co. v. Rosebud Sioux Tribal Court, 133 F.3d 1087 (8th Cir. 1998) (involving the descendants of the Sioux leader Crazy Horse, then 115 years dead, trying to use right of publicity law to stop the marketing of Crazy Horse Malt Liquor; the malt liquor company won on procedural grounds).

[19] Corliss v. E.W. Walker Co., 64 F. 280, 282 (C.C.D. Mass. 1894).

[20] *See, e.g.,* Kaiser Aetna v. United States, 444 U.S. 164, 179-80 (1979) ("the 'right to exclude' [is] universally held to be a fundamental element of the property right").

[21] *See, e.g.,* New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964); *see also* Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (same as to intentional infliction of emotional distress); NAACP v. Claiborne Hardware, 458 U.S. 886 (1982) (same as to intentional interference with business relations).

[22] *See, e.g.,* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy,* 84 GEO. L.J. 2381, 2393 (1996).

[23] *See generally, e.g.,* Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore,* 1999 STAN. TECH. L. REV. VS 8, *available at* <http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8/> (concluding that traditional intellectual property law provides little support for informational privacy speech restrictions); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1136-46 (2000) (same).

[24] 471 U.S. 539 (1985).

view of the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and *uncopyrightable facts* and ideas," copyright law is constitutional. Under the copyright exception to free speech protection, then, speech that borrows creative expression is restrictable, but speech that borrows only facts remains free.

The same goes for other intellectual property rights in speech, such as trademark law, right of publicity law, and trade secret law. For space reasons, I will not discuss them in detail here; a thorough discussion is available in Parts III.B.2-4 of http://www.law.ucla.edu/faculty/volokh/privacy.htm. But the bottom line is that all these restrictions create a fairly narrow right that may affect the form of people's speech but ought not prevent people from communicating facts. Any putative property right in one's personal information can thus be adopted by analogy only if one is willing to relax this limitation, a limitation that is critical to protecting free speech.

C. Functional Arguments for Upholding Information Privacy Speech Restrictions Under a Property Theory

1. *Avoiding "free-riding" and unjust enrichment.*

Some argue for property rights in personal information on functional grounds: Those who communicate personal information about others are engaging in a sort of free riding, enriching themselves without compensating the people whose existence makes their enrichment possible; and property rights, the argument goes, are the way to avoid this free riding. As one article argued, in 1988 three leading credit bureaus made almost $1 billion put together from selling credit information, but "[h]ow much did these credit bureaus pay consumers for the information about them that they sold? Zero." [25]

This, though, cannot be the justification for restricting speech, unless we are willing to dramatically redefine free speech law. Newspapers and radio and TV news programs, after all, make billions from stories that are made possible only by the existence of their subjects.

The essence of news is precisely the reporting of things done or discovered by others; the essence of the news business is profiting from reporting on things done or discovered by others. But news organizations generally don't pay a penny to the subjects of their stories—in fact, it is seen as unethical for news organs, though not entertainment organs, to pay subjects. Likewise, unauthorized biographers and historians make money from publishing information about others, information that only exists because those people exist. Comedians who tell jokes about people make a living from those they mock.[26]

All these speakers are free-riding: They are taking advantage of something that relates to someone else and that exists only because of that other person's existence, and they aren't paying that person for it (though they are usually investing a good deal of time, money, and effort in the project—this free-riding is certainly not mere literal copying). But our legal system correctly allows a great deal of free-riding. It has never been a principle of tort law that all free-riding is illegal, or that all such enrichment is unjust.

Intellectual property law has generally tried to prevent not free-riding as such, but free-riding of a particular kind: the use not just of something that relates to another, but the use of the product of another's substantial labor, and even that only in limited cases. Such a use runs the risk of dramatically diminishing the in-

---

[25] Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment,* 80 CORNELL L. REV. 1756, 1793 (1995).

[26] In some of these examples, some subjects of the speech do profit from the speech, albeit indirectly. The subject of a story may be pleased by his newfound fame; the manufacturer of a product that's covered favorably in the newspaper may make money as a result of the coverage. But of course other subjects of news stories are hurt, either financially or emotionally, by those stories; in such cases, the news organ may be making a profit at the same time that the subjects of the stories, without whom the stories would never have existed, are suffering a loss. Free speech law's response to these subjects is "tough luck," at least unless the stories say something false.

And in this respect, distribution of personal information databases is no different from the publishing of news. Many, perhaps most, of the subjects of these databases derive indirect benefits just like the subjects of news stories do. If I have a good credit history, I am benefited by the credit history databases—if the databases didn't exist and would-be creditors had no way of knowing my record, I'd have to pay a higher interest rate. Likewise, while many people are annoyed by having their personal information available to marketers, some people apparently find the targeted marketing useful, or else they wouldn't buy as a result of this marketing and the marketing would become unprofitable and stop. Thus, some (but not all) people indirectly benefit as a result of information about them being stored in databases—just as some (but not all) people indirectly benefit as a result of news stories about them or their businesses.

centive to engage in such labor, which is what makes the defendant's enrichment socially harmful rather than merely unjust in some abstract moral sense.

This concern is at the heart of copyright law,[27] of the right to prevent the unauthorized transmission of an entire act,[28] and to a large extent of trade secret law. But this concern does not apply to personal information about people, where the incentive arguments don't really apply.

2. *Internalizing costs and maximizing aggregate utility.*

Another functional argument often made on behalf of a property rights theory of information privacy speech restrictions is that the property rights model is the best way to require speakers to "internalize th[e] cost" of their speech "by paying those whose data is used."[29] Such internalizing, the theory goes, would maximize aggregate social utility: By "recogniz[ing the] diversity" of people's desires for information privacy, the property rule could make sure that information about each person is communicated only if the benefit to the speaker exceeds the felt cost to the subject.[30]

The principle of free speech law, though, is that speakers do *not* have to internalize all the felt costs that flow from the communicative impact of their speech. The NAACP didn't have to internalize the tangible economic (not just emotional) cost that its boycott imposed on the Claiborne County merchants.[31] Movie producers don't have to internalize the tangible cost that their movies impose on victims of viewers who commit copycat crimes.[32] Cohen, Johnson, and Hustler didn't have to internalize the emotional distress cost that their speech inflicted on passersby or on its subject.[33]

D. The Potential Consequences

Of course, despite the arguments given above, the Court is always free to broaden the intellectual property exception to allow people to restrict facts; but this, I think, would be a bad idea.

Speech that reveals private information is not the only speech that some want to restrict under the property rights model. As many leading commentators have recently argued, we are now in the midst of a broad movement that uses intellectual property rhetoric to broaden people's rights to restrict others' speech.[34] The proposed database protection legislation would give database owners a form of property right in collections of information.[35]

Some recent cases have revived the misappropriation tort, recognizing a property right in news.[36] Many recent cases have broadened trademark owners' rights to restrict parodies and other transformative uses (though fortunately some courts seem to be resisting this trend).[37] The right of publicity is growing to include any advertising, merchandising, and even interior decor that reminds people of a celebrity, even if it doesn't use the celebrity's name or likeness.[38]

Many have criticized this creeping propertization of speech, often on First Amendment grounds.[39] But if the arguments that "it's not a speech restriction, it's an intellectual property rule" or "the Supreme Court has upheld property rights in information, so property rights in information are constitutional" are accepted for informa-

---

[27] *See* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349 (1991).

[28] Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 576 (1977).

[29] Lessig, *supra* note 12, at 63.

[30] *See, e.g., id.*; Bloustein, *supra* note 12, at 439-40; Murphy, *supra* note 12, at 2395-96.

[31] NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982).

[32] *E.g.*, Olivia N. v. NBC, Inc., 178 Cal. Rptr. 888 (Ct. App. 1981) (barring recovery where child was sexually abused by minors who allegedly copied a similar crime shown on television).

[33] Cohen v. California, 403 U.S. 15 (1971) (public profanity constitutionally protected); Texas v. Johnson, 491 U.S. 397 (1989) (public flag burning constitutionally protected); Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (vicious personal attack constitutionally protected).

[34] *See, e.g.,* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain,* 74 N.Y.U. L. REV. 354, 354 (1999) ("We are in the midst of an enclosure movement in our informational environment.").

[35] *See id.* at 358, 440, 445-46.

[36] *See, e.g.,* NBA v. Motorola, Inc., 105 F.3d 841, 853 (2nd Cir. 1997) (fortunately limiting the tort to only a narrow range of hot news).

[37] *See generally* Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense,* 108 YALE L.J. 1687 (1999).

[38] *See, e.g.,* White v. Samsung Elecs. Am., Inc., 989 F.2d 1512, 1520 (9th Cir.) (Kozinski, J., dissenting from denial of rehearing en banc); Wendt v. Host Int'l, 125 F.3d 806 (9th Cir. 1997).

[39] *See, e.g.,* Lemley, *supra* note 36, at 1710-12 ("The expansive power that is increasingly being granted to trademark owners has frequently come at the expense of freedom of expression. As trademarks are transformed from rights against unfair competition to rights to control language, our ability to discuss, portray, comment, criticize, and make fun of companies and their products is diminishing.").

tion privacy speech restrictions, they will be considerably strengthened as to the other restrictions, too.

Now perhaps my parade of horribles isn't so horrible; maybe we should have more property rights in facts, which is to say restrictions or speech that communicates facts. Nonetheless, people who are worried about the general trend towards propertization of information should look very carefully at even those proposals that might at first seem benign and even just; such proposals could have effects far beyond the context in which they are first suggested.

IV. COMMERCIAL SPEECH

A. What "Commercial Speech" Means

Some argue that sale of information about customers is restrictable because it fits within the "commercial speech" doctrine.[40] The Court's definition of "commercial speech," though, isn't (and can't be) simply speech that is sold as an article of commerce: Most newspapers, movies, and books are articles of commerce, too, but they remain fully protected.[41] Likewise, speech can't be commercial just because it relates to commerce, or else the *Wall Street Journal,* union leaflets and newsletters,[42] newspaper reviews of commercial products,[43] and speech by disgruntled consumers criticizing what they consider poor service by producers would be deprived of full constitutional protection.

Rather, the Court's most now-standard definition of commercial speech is speech that explicitly or implicitly "propose[s] a commercial transaction."[44] Commercial advertisements for products or services are classic examples. So are stock prospectuses, which propose the purchase of stock; this is why fairly heavy SEC regulation of speech in such prospectuses is largely permissible, while similar SEC regulation of newsletters or newspapers that discuss stocks is not.[45]

Under the "speech that proposes a commercial transaction" analysis, communication of information about customers by one business to another is not commercial speech. It doesn't advertise anything, or ask the receiving business to buy anything from the communicating business.[46] It poses no special risk of the speaker misleading or defrauding the listener, beyond those risks present with fully protected speech generally. The recipient business does intend to use the information to more intelligently engage in commercial transactions, but that's equally true of businesspeople reading *Forbes.*

Of course, even if speech that communicates personal information is seen as "commercial speech," restrictions on such speech will still have to face considerable scrutiny. Whether they will pass such scrutiny is hard to tell, since commercial speech scrutiny is so notoriously vague. But this question is actually somewhat tangential to my main point. To me, the main problem with treating speech that communicates personal information as "commercial speech" is not that this will put such speech at more risk of restriction. Rather, it is that stretching the definition of "commercial speech" will put a wide range of other speech at risk, too.

B. The Risks to Other Speech

Consider a recent example of the government trying to regulate cyberspace speech about economic matters on the grounds that it's "commercial speech." In *Taucher v. Born,* several operators of commodities-themed Web sites successfully sued to set aside a prior restraint system which bars people from distributing for profit any unlicensed speech that relates "to the value of or the advisability of commodity trading" or that contains "analyses or reports" about commodities.[47]

And the license that speakers must get to be allowed to speak isn't just a modest tax; the Commodities Futures Trading Commission can refuse a license if it finds "good cause" to do so, and speaking without a license is illegal. Nor is this speech

---

[40] *See, e.g.,* United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133, 1137 (9th Cir. 1999), *rev'd on other grounds sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999).

[41] *See, e.g.,* Smith v. California, 361 U.S. 147, 150 (1959) ("It is of course no matter that the dissemination [of speech by the claimant] takes place under commercial auspices").

[42] *See, e.g.,* Debartolo Corp. v. Florida Gulf Coast Trades Council, 485 U.S. 568 (1988).

[43] *See, e.g.,* Bose Corp. v. Consumers Union, 466 U.S. 485 (1984).

[44] Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 761 (1976).

[45] *See* Lowe v. SEC, 472 U.S. 181, 211 (1985) (White, J., concurring in the judgment).

[46] Sometimes, of course, a business will use customer information that it has bought from another business to send out commercial advertisements to prospective clients. These advertisements would indeed be commercial speech, though the original communication of the customer information is not. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

[47] 7 U.S.C. § 6m(1).

restriction limited to individualized, person-to-person professional advice: The regulation is broad enough to cover people who "never engage in individual consultations with their customers" and who "under no circumstances make trades for their customers."[48]

The law essentially restricts the Web equivalent of books and newspapers about commodity training—it's as if the government claimed the right to refuse the *Wall Street Journal* a license to publish articles about the market. As it happens, the law specifically excludes publishers who publish such data "incidental[ly]" as part of a broader news enterprise of "general and regular dissemination,"[49] so the *Journal* can sleep easy. But under the logic of the law, newspapers and book publishers could also be subject to a prior restraint system, just as the small commodities-focused electronic publishers were subject to it until the court's ruling.

The CFTC argued that speech about commodities is mere "commercial speech," but the court correctly rejected this:[50] "The plaintiffs' publications in this case do not propose any commercial transaction between the plaintiffs and their customers."[51] If, however, the commercial speech doctrine had been extended to cover the sale of speech about a business's clients, the court's decision might well have been different.

After all, the Web business journalist who writes about commodities is likewise selling information that's primarily of economic concern, and that has little to do with broad political debates. If that's enough to deny free speech protection to communications about customers, it may be enough to deny such protection to communications about commodities.

Consider another example: disgruntled homebuyers putting up signs criticizing the developer that sold them their homes, or consumers leafleting outside a business that they claim sold them defective goods, often hoping that the business will give them a refund or at least will do a better job in the future. In cyberspace, the analogy would be consumers putting up a http://www.[businessname]sucks.com site or circulating messages to a long list of acquaintances or to a Usenet newsgroup.

In my view, the First Amendment fully protects such speech that is aimed at creating public pressure on someone to do what you think is right, even in economic contexts—that, after all, is what much advocacy is about.[52] The fact that the speech exposes alleged problems with a product and aims at redressing an economic harm should not strip it of protection. For many people problems with their homes and redress for shoddy wares are more important than problems with politicians and redress for shoddy policies, and far more important than art, entertainment, or many other kinds of fully protected speech.

If the consumer's speech is an intentional lie (or perhaps in some circumstances if it's merely negligently false), the business can sue for libel; false statements of fact, whether on economic matters or not, lack constitutional protection. But the law shouldn't impose extra restrictions on the speech just because the speech deals with economic issues.

Again, though, a broadening of the commercial speech doctrine would jeopardize speech of this sort. If communicating information about a person's bad credit record is mere "commercial speech," then communicating information about a business's bad service record should be, too.

Both, after all, involve speech on economic matters. Both involve speech that's primarily of economic interest to listeners. Both are motivated by the speaker's economic interest—either a desire to get money from the buyer of the information, or a desire to get redress from the business. Either both are commercial speech or neither is.

In a free and competitive economy, people naturally want to talk about economic matters. Giving the government an ill-defined but potentially very broad power to restrict such speech—not just speech that proposes a commercial transaction be-

---

[48] Taucher v. Born, 53 F. Supp. 464, 478 (D.D.C. 1999).

[49] 7 U.S.C. §§ 1a(5)(B)(iv), 1a(5)(C).

[50] The CFTC's other argument was that the government may regulate speech in the context of a professional-client relationship, but the court adopted the response to a similar argument given by Justice White in his *SEC v. Lowe,* 472 U.S. 181 (1985), concurrence: Whatever extra power the government may have to regulate the professional-client relationship, this power arises only when the professional exercises individualized judgment on behalf of a particular client. Personal advice may to some extent be restricted, but books, newsletters, and the like may not be.

[51] *Taucher v. Born,* 53 F. Supp. at 480.

[52] *See, e.g.,* Debartolo Corp. v. Florida Gulf Coast Trades Council, 485 U.S. 568 (1988); NAACP v. Claiborne Hardware, 458 U.S. 886 (1982); Keefe v. Organization for a Better Austin, 402 U.S. 415 (1971).

tween speaker and listener and thus directly implicates the risk of fraud—risks exposing a great deal of speech to government policing.

V. SPEECH ON MATTERS OF PRIVATE CONCERN

A. The Argument

One feature of virtually all information privacy proposals (except those built on a contract model) is their distinction between speech on matters of public concern and speech on matters of private concern.[53] Even people who argue that newspapers should be forbidden from publishing a private person's long-ago criminal history or a politician's sexual orientation would probably agree that they have a right to publish the politician's criminal history, no matter how old. "Political speech" or "speech on matters of public concern" or "newsworthy" material, they would argue, is constitutionally protected, while speech that is merely of private concern is not protected, at least against information privacy speech restrictions.

But this approach, I will argue, is theoretically unsound; it is precedentially largely unsupported; in the few circumstances in which it has been endorsed, it has proven unworkable; and, if adopted, it would strengthen the arguments for many other (in my view improper) speech restrictions.

B. The Dangers of the Argument

Under the First Amendment, it's generally not the government's job to decide what subjects speakers and listeners should concern themselves with.[54] A private concern exception essentially says "you have no right to speak about topics that courts think are not of legitimate concern to you and your listeners," a view that's inconsistent with this understanding.

A clear example of the danger of such government power comes in a disclosure tort case, *Diaz v. Oakland Tribune*.[55] Diaz, the first woman student body president at a community college, was a transsexual, and the Oakland Tribune published this fact. Diaz sued, and the court of appeals held that her lawsuit could go forward; if a jury found that Diaz's transsexuality wasn't newsworthy, she could prevail.[56]

As usually happens in these cases, the court didn't define newsworthiness but left it to the jury, subject only to the instruction that "[i]n determining whether the subject article is newsworthy you may consider [the] social value of the fact published, the depth of the article, [its] intrusion into ostensibly private affairs, and the extent to which the plaintiff voluntarily acceded to a position of public notoriety." But the court did stress that a jury could find that the speech wasn't newsworthy: "[W]e find little if any connection between the information disclosed and Diaz's fitness for office. The fact that she is a transsexual does not adversely reflect on her honesty or judgment."

Now I agree with the court's factual conclusion; people's gender identity strikes me as irrelevant to their fitness for office. But other voters take a different view. Transsexuality, in their opinion, may say various things about politicians: It may say that they lack attachment to traditional values, that they are morally corrupt, or even just that they have undergone an unnatural procedure and therefore are somehow tainted by it.

These views may be wrong, but surely it is not for government agents—whether judges or jurors—to dictate the relevant criteria for people's political choices, and to use the coercive force of law to keep others from informing them of things that they may consider relevant to those choices. I may disagree with what you base your vote on, but I must defend your right to base your vote on it, and the right of others to tell you about it.

This is the clearest example of a court using the public concern test to usurp what should be a listener's and speaker's choice, but other public disclosure cases raise similar problems. Consider, for instance, the criminal history cases, in which some courts held that it was illegal for newspapers to print information about "long past" criminal activity by people who are now supposedly rehabilitated and are leading

---

[53] *See, e.g.,* among many others, Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black,* 68 TEX. L. REV. 1195, 1229-30 (1990); Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1414, 1417 (2000).

[54] *See, e.g.,* Police Dep't v. Mosley, 408 U.S. 92, 95 (1972) ("[A]bove all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."). The Court has recognized some exceptions to this principle, but this presumption is still the basis for the Court's analysis of speech restrictions imposed by the government as sovereign.

[55] 188 Cal. Rptr. 762 (Ct. App. 1983).

[56] The court set aside the verdict for Diaz because of a jury instruction error, but remanded for a new trial.

allegedly blameless lives. The leading such case is *Briscoe v. Reader's Digest Association,* in which *Reader's Digest* was held liable for revealing that Briscoe had eleven years earlier been convicted of armed robbery (a robbery that involved his fighting "a gun battle with the local police").[57]

The court acknowledged that the speech, while not related to any particular political controversy, was newsworthy; the public is properly concerned with crime, how it happens, how it's fought, and how it can be avoided. Moreover, revealing the identity of someone "currently charged with the commission of a crime" is itself newsworthy, because "it may legitimately put others on notice that the named individual is suspected of having committed a crime," thus presumably warning them that they may want to be cautious in their dealings with him.

But revealing Briscoe's identity eleven years after his crime, the court said, served no "public purpose" and was not "of legitimate public interest"; there was no "reason whatsoever" for it. The plaintiff was "rehabilitated" and had "paid his debt to society." "[W]e, as right-thinking members of society, should permit him to continue in the path of rectitude rather than throw him back into a life of shame or crime" by revealing his past.

"Ideally, [Briscoe's] neighbors should recognize his present worth and forget his past life of shame. But men are not so divine as to forgive the past trespasses of others, and plaintiff therefore endeavored to reveal as little as possible of his past life." And to assist Briscoe in what the court apparently thought was a worthy effort at concealment, the law may bar people from saying things that would interfere with Briscoe's plans.

Judges are of course entitled to have their own views about which things "right-thinking members of society" should "recognize" and which they should forget; but under the First Amendment, members of society have a constitutional right to think things through in their own ways.

And some people do take a view that differs from that of the *Briscoe* judges: While criminals can change their character, this view asserts, they often don't. Someone who was willing to fight a gun battle with the police eleven years ago may be more willing than the average person to do something bad today, even if he has led a blameless life since then (something that no court can assure us of, since it may be that he has continued acting violently on occasion, but just hasn't yet been caught).

Under this ideology, it's perfectly proper to keep this possibility in mind in one's dealings with the supposedly "reformed" felon. While the government may want to give him a second chance by releasing him from prison, restoring his right to vote and possess firearms, and even erasing its publicly accessible records related to the conviction, his friends, acquaintances, and business associates are entitled to adopt a different attitude.

Most presumably wouldn't treat him as a total pariah, but they might use extra caution in dealing with him, especially when it comes to trusting their business welfare or even their physical safety (or that of their children) to his care.[58] And they might use extra caution in dealing with him precisely because he has for the last eleven years hidden this history and denied them the chance to judge him for themselves based on the whole truth about his past.[59] Those who think such concealment is wrong will see it as direct evidence of *present* bad character (since the concealment was continuing) and not just of past bad character.

Revealing Briscoe's name, under this view, may have little to do with broad political debates, but it is still of intense and eminently legitimate public concern to one piece of the public: people who know Briscoe, the very same group whose ignorance Briscoe seemed most concerned about preserving. These members of the public would use this information to make the decision, which is probably more important to them than whom they would vote for next November, about whether they could trust Briscoe in their daily dealings.

This isn't speech on political matters, but rather on what I might call "daily life matters." Under the First Amendment, which protects movies, art, jokes, and re-

---

[57] 483 P.2d 34, 36 (Cal. 1971).

[58] If you were deciding whether to leave your children for the day in a neighbor's care, would you consider his eleven-year-old conviction for a violent crime involving a gun battle with police relevant (not necessarily dispositive, but relevant) to your decision? Would you advise your daughter to consider a prospective date's armed robbery conviction when deciding whether and under what conditions to go out with him?

[59] Richard A. Epstein, *Privacy, Property Rights, and Misrepresentations,* 12 GA. L. REV. 455, 472-73 (1978).

views of stereo systems,[60] such speech on daily life matters is at least equally worthy.

At least as much as those kinds of protected speech, daily life matter speech—communication related to "the real, everyday experience of ordinary people"[61]—indirectly but deeply affects the way we view the world, deal with others, evaluate their moral claims on us, and even vote; and its effect is probably greater than that of most of the paintings we see or the editorials we read. Consider how much our view of crime and punishment, secrecy and publicity, and many other topics would be indirectly influenced—towards greater liberalism, conservatism, or something else—by the knowledge that some of our seemingly law-abiding neighbors have been concealing a criminal past.

In any event, which viewpoint about our neighbors' past crimes is "right-thinking" and which is "wrong-thinking" is the subject of a longstanding moral debate. Surely it is not up to the government to conclude that the latter view is so wrong, that Briscoe's conviction was so "[il]legitimate" a subject for consideration, that the government can suppress speech that undermines its highly controversial policy of forgive-and-forget.

This also goes for databases of personal information as much as for news stories about such information. Many such databases—for instance, credit history databases or criminal record databases—are used by people to help them decide whom it is safe to deal with and who is likely to cheat them.

Other databases, which contain less incriminating information, such as a person's shopping patterns, may be less necessary for self-protection; but of course for the same reason the data stored in them will also generally be much less embarrassing to their subjects, which makes the supposed harm to the subjects of the communication of such data much smaller. And in any event, even this data is of direct daily life interest to its recipients, since it helps them find out with whom they should do business.

In some instances, it may be quite unlikely that certain speech would be useful to the listeners either for political purposes or for daily life purposes; this largely has to do with information that shows people in ridiculous, embarrassing, or demeaning contexts without revealing any useful new information about them. Everybody knows that I go to the bathroom; printing a picture of me on the toilet would embarrass me not because it reveals something new about me, but because it shows me in a pose that by cultural convention is seen as ridiculous or undignified.

But while there may be a narrow zone of fairly uncontroversially non-public-concern topics, the danger is that the vague, subjective "public concern," "newsworthiness," or "legitimate public interest" test will flow far beyond this zone; and as *Briscoe* and *Diaz,* among others, show, this danger has materialized. This risk may be enough to abandon the test altogether, and it is certainly enough to demand that the test be rephrased as something much clearer and narrower before it is accepted.

We can all think of examples of entertainment that has no connection to public issues, but *Winters v. New York* was right to conclude that entertainment should be protected despite this, because "[t]he line between the informing and the entertaining is too elusive for the protection of [the] basic right [of free speech]."[62] If vitriolic, relatively nonsubstantive parodies such as the one in *Hustler v. Falwell* were banned, "public discourse would probably suffer little or no harm," but the Court correctly refused to uphold such a ban, since it could find no "principled standard to separate" them from speech that had to be protected.[63]

Likewise, the notion that speech should generally be restrictable when it doesn't relate to matters of public concern strikes me as so potentially broad and so vague that it deserves to be abandoned, even if it would yield the right results in a narrow subset of the cases in which it would be applied.

C. Doctrine

That, then, is why I think the public concern test is theoretically unsound. The doctrinal discussion is easier: Though the Court has often said in dictum that political speech or public-issue speech is on the "highest rung" of constitutional protec-

---

[60] *See, e.g.,* Winters v. New York, 333 U.S. 507 (1948) (entertainment); Bose Corp. v. Consumers Union, 466 U.S. 485 (1984) (product review of stereo equipment); Abood v. Detroit Bd. of Educ., 431 U.S. 209, 231 (1977) ("[O]ur cases have never suggested that expression about philosophical, social, artistic, economic, literary, or ethical matters—to take a nonexhaustive list of labels—is not entitled to full First Amendment protection.").

[61] Cynthia L. Estlund, *Speech on Matters of Public Concern: The Perils of an Emerging First Amendment Category,* 59 GEO. WASH. L. REV. 1, 37 (1990).

[62] 333 U.S. 507, 510 (1948).

[63] . 485 U.S. 46, 55 (1988).

tion,[64] it has never created any general exception for speech on matters of "private concern." Political speech, scientific speech, art, entertainment, consumer product reviews, and speech on matters of private concern are thus all doctrinally entitled to the same level of high constitutional protection, restrictable only through laws that pass strict scrutiny.

The two situations where the Court has adopted a public concern / private concern distinction are narrow exceptions to this general principle. The first such exception, established in *Connick v. Myers,* is that the government acting as employer may freely restrict speech on matters of private concern by its employees.[65]

The government's power as employer to fire its employees for what they say has always been far greater than its power to fine or imprison private citizens for what they say, and the *Connick* Court explicitly stressed that private-concern speech remains protected against the government acting as sovereign.[66] The restriction on such speech by government employees was justified only by the special role of the government acting as employer, in which the government's interest in efficient day-to-day operation would make it infeasible to let people sue the government over every discharge that was based on any sort of speech.

The second exception, established in *Dun & Bradstreet v. Greenmoss Builders,* is that plaintiffs in libel cases involving false statements on matters of purely private concern may be awarded punitive and presumed damages without a showing of actual malice.[67] This, though, also came in a context where the government has special power to restrain speech: restrictions on false statements of fact.

Such statements, the Court has held, have "no constitutional value"; any protection they get stems from the need to prevent the undue chilling of true statements, which are indeed constitutionally protected.[68] The economic interests of the speaker and its audience, the Court argued, warrant no special protection when "*the speech is wholly false.*"[69] *Dun & Bradstreet* thus says little about the propriety of applying the "private concern" test to speech that, unlike false statements of fact, is presumptively constitutionally valuable.[70]

D. The Experience Under the Two "Public Concern" Doctrines

In practice, neither of these doctrines has been a success story for the public concern test. As many critics have pointed out, the government employee private concern doctrine has proven both vague to the point of indeterminacy and extremely broad.[71] Much speech that would clearly fit within a normal reading of the words "public concern" has been found to be of purely private concern and therefore unprotected, with seemingly little justification other than the desire to make life easier for government employers confronted with troublemaking employees.

Connick itself found that speech among District Attorney's office employees about "the confidence and trust that [employees] possess in various supervisors, the level of office morale, and the need for a grievance committee" was "not of public concern," hardly a commonsense reading of the term "public concern."

Later cases have likewise found, for instance, that speech criticizing the way a dean runs a public university department,[72] alleging race discrimination by a public employer,[73] and criticizing the way the FBI decides whom to lay off[74] was not "of public concern," though other cases reached opposite results on seemingly similar facts.[75] Whether or not the government should have the power to dismiss employees for such speech, surely the government ought not have the power to censor such

---

[64] Carey v. Brown, 447 U.S. 455, 467 (1980).

[65] 461 U.S. 138 (1983).

[66] "We in no sense suggest that speech on private matters falls into one of the narrow and well-defined classes of expression which carries so little social value, such as obscenity, that the State can prohibit and punish such expression by all persons in its jurisdiction [and not just its own employees]." *Id.* at 147.

[67] 472 U.S. 749 (1985).

[68] *Id.* at 767 (White, J., concurring in the judgment). *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 340-41 (1974).

[69] *Dun & Bradstreet*, 472 U.S. at 762 (emphasis added).

[70] *Cf., e.g.,* U.D. Registry, Inc. v. California, 40 Cal. Rptr. 2d 228, 232 (Ct. App. 1995) ("While the distinction [between private and public concern speech] may be significant in the area of defamation, it does not define the parameters of permissible regulation for truthful reporting.").

[71] *See, e.g.,* Stephen Allred, *From Connick to Confusion: The Struggle to Define Speech on Matters of Public Concern,* 64 IND. L.J. 43 (1988); Estlund, *Speech on Matters of Public Concern, supra* note 60, at 7 n.40, 34, 45.

[72] Landrum v. Eastern Ky. Univ., 578 F. Supp. 241 (E.D. Ky. 1984).

[73] Lipsey v. Chicago Cook County Criminal Justice Comm'n, 638 F. Supp. 837 (N.D. Ill. 1986).

[74] Murray v. Gardner, 741 F.2d 434 (D.C. Cir. 1984).

[75] *See generally* Allred, *supra* note 70, at 65-73.

speech by citizens at large on the grounds that it's supposedly of insufficient "public concern."

Under *Dun & Bradstreet,* the concept of "speech of purely private concern" has ended up similarly vague, and has sometimes covered speech that clearly seems to be of public concern under any normal definition of the term: for instance, speech discussing the competence of psychologists to whom children are sent by government-run schools, the business practices of car dealers, and alleged misconduct by the owner of a gymnastics school.[76] Again, perhaps it's permissible to allow presumed and punitive damages for *false* statements on such topics, but surely it would be unconstitutional to restrict *true* statements on these matters on the grounds that they aren't of "public concern."

The experience of the public concern test in these two areas thus suggests that the theoretical criticisms of the public concern / private concern distinction are sound: There's a substantial practical risk of the courts finding too much speech to be of "private concern," and while some facially vague and broad tests have the merit of being tied to an existing body of clarifying and narrowing caselaw, that's hardly the case here.

Maybe for lack of anything better, the public / private concern distinction may remain sensible as to the genuinely hard and necessarily vague government employee speech cases, but its track record hardly seems to encourage expanding it elsewhere.

E. Potential Consequences

All this discussion is not just academic or just applicable to information privacy speech restrictions. The argument that certain speech should be more restrictable because it's not "political speech," not "high-value speech," or not of "legitimate public interest" is routinely marshaled in favor of a broad range of speech restraints.

Businesses criticized by disgruntled consumers have already argued that such consumer criticism doesn't relate to speech on matters of genuinely "public concern," and should therefore be restrictable even if it's true or if it's mere opinion.[77] Likewise, supporters of campus speech codes have argued that this speech too, is of low value.[78] Allowing tort liability under the disclosure tort for speech on supposedly "private matters" (such as a person's criminal history or failure to pay his debts[79]) would provide strong support for allowing tort liability under the intentional interference tort for speech on "private matters" (such as a business's unfair practices or breaches of warranty), or for allowing universities to suppress speech that they find supposedly valueless.

VI. COMPELLING INTEREST

The last argument for many proposed information privacy speech restrictions is that the government interest behind the restriction is just so great. Speech that reveals personal information about others, the argument goes, violates their basic human rights, strips them of their dignity, causes serious emotional distress, interferes with their relations with family, friends, acquaintances, and business associates, and puts them at risk of crime.

Moreover, such speech itself undermines other rights of constitutional stature, such as the right to privacy or free speech itself. The government must be able to step in and prevent this, even at the cost of creating a new free speech exception.

A. Countervailing Constitutional Rights

Let me begin by discussing the "constitutional tension" argument, which comes in two flavors: (1) Because the Constitution has been interpreted as protecting privacy (possibly including information privacy[80]), attempts to restrict speech in the name of protecting information privacy involve a "tension" between two constitutional values.[81] (2) Information privacy speech restrictions "promote[] some of the same values protected by the First Amendment," because "[g]ranting people privacy, recognizing that despite their entering into the public debate on an issue . . . they re-

---

[76] *See* Robert E. Drechsel, *Defining "Public Concern" in Defamation Cases Since Dun & Bradstreet v. Greenmoss Builders,* 43 FED. COMM. L.J. 1, 17-18 (1990); Saunders v. Van Pelt, 497 A.2d 1121 (Me. 1985); Vern Sims Ford, Inc. v. Hagel, 713 P.2d 736 (Wash. Ct. App. 1986); Ramirez v. Rogers, 540 A.2d 475 (Me. 1988).

[77] *See, e.g.,* Paradise Hills Assocs. v. Procel, 1 Cal. Rptr. 2d 514, 521 (Ct. App. 1991).

[78] *See, e.g.,* Richard Delgado, *Campus Antiracism Rules: Constitutional Narratives in Collision,* 85 Nw. U. L. REV. 343 (1991).

[79] *See, e.g.,* Mason v. Williams Discount Ctr., Inc., 639 S.W.2d 836 (Mo. Ct. App. 1982).

[80] *See* Whalen v. Roe, 429 U.S. 589, 605 (1977).

[81] *See also* Melvin v. Reid, 112 Cal. App. 285, 291 (1931).

main a private person to some degree, encourages people to come forward and engage in the debate."[82]

I have elsewhere argued at length against this sort of analysis,[83] but for now let me make two observations about it. First, the speech vs. privacy and speech vs. speech tensions are not tensions between constitutional rights on both sides. The Constitution presumptively prohibits government restrictions on speech and perhaps some government revelation of personal information, but it says nothing about interference with speech or revelation of personal information by nongovernmental speakers.

If, for instance, a private group organizes a boycott of a newspaper to pressure it into dropping a columnist whose work the group finds offensive,[84] the group is not thereby violating the columnist's First Amendment rights; he has a constitutional right to speak free from government restraint, but not free from private censure or private pressure.

Likewise, information privacy speech restrictions involve a tension between a *constitutionally secured* right to speak free of government restriction and a proposed *statutory or common-law* right to speak free of private revelation of private information. The fact that the proposed statutory or common-law right is in one way analogous to a constitutional right does not give it constitutional stature.

Second, as the boycott example shows, changing First Amendment doctrine to let free speech rights be trumped by other "constitutional values" derived by analogy from constitutional rights would permit a broad range of speech restrictions. Lots of speech has the effect, and often the purpose, of discouraging people from exercising their speech rights in certain ways.

Political bullies try to silence their opponents not only by revealing embarrassing private information about them, but also by calling them nasty (but nonlibelous) names, citing their interracial marriages as evidence that they are traitors to their race,[85] attacking them with bitter and unfair parodies, or saying things aimed at undermining their business affairs.

Depending on the era, the risk of having your arguments called "Communist," "un-American," "racist," or "sexist" (even if your arguments really don't fall into those categories) has discouraged many people from expressing viewpoints that might draw such rhetoric—and I suspect that the rhetoric was often used precisely to deter people from expressing certain viewpoints. Who among us hasn't at times decided to stay quiet in order to avoid having to deal with our opponents' vituperation?

The logic of the argument I quoted, if accepted, would thus justify restriction on all these kinds of speech. And yet our right to use speech to pressure others into not speaking is a fundamental aspect of the First Amendment; recall that a recurring (and correct) argument of those who fight against advocacy of evil ideas—even advocacy that is concededly constitutionally protected against government suppression—is that such speech should be deterred by social ostracism and condemnation.

Likewise, accepting the other constitutional tension argument, which urges that speech be restricted when it undermines the unwritten constitutional "value" of privacy, would provide strong support for restrictions on speech that vehemently criticizes a religion and thereby discourages people from publicly adhering to it (and thus supposedly undermines the explicitly constitutionally described values of religious freedom),[86] speech that urges people to treat others unequally (and thus undermines equality), speech that tries to pressure people into not exercising their property or contractual rights (and thus undermines private property rights or the

---

[82] Sean M. Scott, *The Hidden First Amendment Values of Privacy,* 71 WASH. L. REV. 683, 687, 710 (1996). *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 VAND. L. REV. 1609, 1701-02, 1651 (1999).

[83] Eugene Volokh, *Freedom of Speech and the Constitutional Tension Method,* 3 U. CHI. L. SCH. ROUNDTABLE 223 (1996).

[84] *See, e.g.,* Jill Stewart, *Free This Man; Can Black Conservatives Speak Their Minds in America? Ask KABC Talk-Show Host Larry Elder, the Target of a Black Nationalist Group in L.A.,* NEW TIMES (L.A.), July 3, 1997 (describing boycott of sponsors of black conservative talk show host Larry Elder's radio show, aimed at getting the radio station to take him off the air); James Warren, *Andy Rooney Suspended, But Denies Racist Comment,* CHI. TRIB., Feb. 9, 1990, § 1, at 3 (describing public pressure that caused CBS to suspend *60 Minutes* commentator Andy Rooney for allegedly making a racist comment); Jerry Berger, *Kennedy Decries Reagan Civil Rights Policies,* United Press Int'l, Jan. 18, 1988, *available in* LEXIS, News Library, UPI File (describing public pressure that caused CBS to fire Jimmy "The Greek" Snyder on similar grounds).

[85] *See, e.g.,* Amy Wallace, *He's Either Mr. Right or Mr. Wrong,* L.A. TIMES, Mar. 31, 1996, at 12.

[86] *Cf., e.g.,* Kunz v. New York, 340 U.S. 290, 295, 302 (1951) (Jackson, J., dissenting).

obligation of contracts), and so on.[87] A rule that constitutional rights to protection from the government may be turned into justification for government restrictions on speech by private actors would have a broad effect indeed.

B. Dignity, Emotional Distress, and Civil Rights

Other arguments for information privacy speech restrictions claim that the speech injures people's dignity or emotionally distresses them. This injury is sometimes also characterized as an interference with people's basic "civil right" not to have others know or say certain things about them.[88]

But is it constitutional for the government to suppress certain kinds of speech in order to protect dignity, prevent disrespectful behavior, prevent emotional distress, or to protect a supposed civil right not to be talked about? Under current constitutional doctrine, the answer is generally no: Even offensive, outrageous, disrespectful, and dignity-assaulting speech is constitutionally protected.[89]

And there is good reason for this approach. If the government can declare it to be my "civil right" to prohibit others from saying the truth about me behind my back, then the arguments for many speech restrictions would be considerably strengthened. The government could similarly declare it a civil right to have others not say insulting things about me (and my kind) in print or in broadcasts, where I may directly see or hear such speech; other countries have indeed done this.

Similarly, say that *true* statements—statements about past crimes, current sexual orientation, credit history, and the like—can be restricted because of the danger that they will change people's attitudes about their subject. Why wouldn't sociological or political claims that the government considers false or misleading (group libel or seditious libel)[90] or statements of opinion (general bigoted or antigovernment advocacy) be likewise restrictable, on the grounds that they may change people's attitudes about a group, and that there's a "compelling governmental interest" in preventing such changed attitudes?

It's conceivable that as to some kinds of speech, for instance the revelation of the names of rape victims or the unauthorized distribution of pictures of a person naked or having sex, courts will find that the speech is so valueless and so distressing that there is indeed a compelling interest in restricting it. Though I empathize with the reasons for such restrictions, I reluctantly oppose them, precisely because of the dangers discussed in Part V and earlier in this section—"lack of legitimate public concern" and "severe emotional distress," while intuitively appealing standards, are so vague and potentially so broad that accepting them may jeopardize a good deal of speech that ought to be protected.

But while these narrow restrictions would merely increase the risk that more speech might be restricted in the future, other proposed restrictions cheerfully embrace this possibility. Broad readings of the disclosure tort would restrict speech about elected officials that many voters would (rightly or wrongly) find quite relevant, or restrict speech about people's past crimes, which many of the people's neighbors may find important.

Likewise, many of the proposals to restrict communication of consumer transactional data would apply far beyond a narrow core of highly private information, and would cover all transactional information, such as the car, house, food, or clothes one buys. I don't deny that many people may find such speech vaguely ominous and would rather that it not take place, and I acknowledge that some people get extremely upset about it. But knowing that some business somewhere knows what car you drive[91] is just not in the same league as, say, knowing that all your neighbors (and thousands of strangers) have heard that you were raped.

If such fairly modest offense or annoyance is enough to justify speech restrictions, then the compelling interest bar has fallen quite low. And watering down the

---

[87] *See generally* Volokh, *supra* note 82, at 231-34, 237-38.

[88] *See, e.g.,* Directive 95/46/EC, art. 1(1) 1995 O.J. (L.281) 31 (describing protection of informational privacy as a matter of "the fundamental rights and freedoms" "of natural persons"); *Talk of the Nation: Online Privacy* (NPR radio broadcast, June 30, 1998) (quoting Todd Lappin, senior associate editor of *Wired* magazine) ("[I]t's really the job of all of us to get a consensus in Congress that'll give us basic legal rights so we have some control over our names and over our personal information. This is a civil rights and a human rights struggle . . .").

[89] *See, e.g.,* Cohen v. California, 403 U.S. 15 (1971) (public profanity); Texas v. Johnson, 491 U.S. 397 (1989) (flag burning); Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (scurrilous, personal attack in print); Brandenburg v. Ohio, 395 U.S. 444 (1969) (racist advocacy); Collin v. Smith, 578 F.2d 1197 (7th Cir. 1978) (Nazi parade in a part of town where many Holocaust survivors lived); Kunz v. New York, 340 U.S. 290 (1951) (vitriolic attacks on Catholicism and Judaism); Cantwell v. Connecticut, 310 U.S. 296 (1940) (vitriolic attack on Catholicism).

[90] *Cf., e.g.,* United States v. Cooper, 25 F. Cas. 631, 639 (C.C.D. Pa. 1800).

[91] *Cf., e.g.,* Gindin, *supra* note 1, at 1157.

threshold for when an interest becomes "compelling" will of course have an impact far beyond information privacy speech restrictions.

C. Keeping the Internet Attractive to Consumers

Some have argued that privacy restrictions are needed to keep Internet access attractive to consumers: Consumers are so concerned that online sites will collect and reveal information about them, the argument goes, that they are being deterred from engaging in e-commerce, and thus e-commerce in particular and the economy in general is suffering.[92]

But fostering economic growth and increasing Internet use, while laudable goals, can hardly be "compelling government interests" justifying content-based bans on certain kinds of speech, at least if the "compelling" threshold is to have any meaning. And the potential consequences of accepting this sort of justification for restricting speech are both clear and dire: The same rationale, after all, would easily justify bans on TV broadcasts that warn of cyberspace privacy risks, since such speech even more directly frightens consumers away from e-commerce and other Internet use.

Furthermore, if this is really such a great concern (which is far from clear, given the explosive growth of e-commerce even in the absence of noncontractual information privacy speech restrictions), it stands to reason that many Internet businesses would invest a lot of effort into preventing such consumer alienation: They'll promise not to communicate consumer information, set up enforcement mechanisms aimed at giving consumers confidence that such promises will be kept, distribute software that helps protect people's privacy through technological means, and so on. The availability of these alternatives further undercuts the case for restricting First Amendment rights in order to protect e-commerce.[93]

D. Preventing Misconduct and Crime

1. *Discrimination.*

Speech that reveals some kinds of information about people may make it easier for the listeners to act illegally or supposedly unfairly towards those people. One commonly given example is the risk that certain health-related information might fall into the hands of your health insurance company. "Say that the insurance company learns that you eat a lot of pizza and steak, and therefore concludes that you'll probably have higher cholesterol and a higher risk of heart disease," the argument goes; "it might then raise your rates." Another example is the risk that information about people's past crimes, alcoholism, or drug abuse will become known to employers, who will then refuse to hire these people.[94]

I can certainly see why people might be offended by their insurance company "snooping" on them this way. I can also see why it might be in the unhealthy eaters' financial interest (and I should mention that I love meat and cheese) not to be identified as such, so they can be subsidized by the healthy eaters with whom they pool their risk. Similarly, closet smokers would prefer, if possible, that life insurance companies not be able to identify them as smokers. But the question is not just whether the communication of this information is offensive or financially costly to its subjects, but rather whether the government may suppress such communication.

If discrimination in insurance based on the insureds' eating habits is legal, as it is with respect to smoking habits, then it's hard to see how the risk of such lawful discrimination can justify restricting speech. True, one's buying habits are not a perfect proxy for one's eating habits (maybe the buyer is a healthy eater who is buying the pizza entirely for his roommate), but insurance is all about using imperfect but lawful predictors.

Being above twenty-five and being a good student don't perfectly predict whether someone will drive safely; smoking and being older don't perfectly predict whether someone will die soon; but virtually nothing perfectly predicts anything else. Likewise, many employers might consider a person's criminal record, alcoholism, or drug

---

[92] *Cf. generally* Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network,* 30 WAKE FOREST L. REV. 105 (1995).

[93] *Cf.* Reno v. ACLU, 521 U.S. 844, 885 (1997) (rejecting on similar though slightly different grounds a similar argument in support of restrictions on sexually themed speech).

[94] *See, e.g.,* James Rachels, *Why Privacy Is Important,* 4 PHIL. & PUB. AFF. 323, 324 (1975) ("Revealing a pattern of alcoholism or drug abuse can result in a man's losing his job or make it impossible for him to obtain insurance protection . . .").

abuse relevant to whether they should entrust their property, their clients' well-being,[95] or a $100 million oil tanker to that person.

But even if the government outlaws discrimination based on insureds' eating habits, or discrimination based on a person's alcoholism, drug use, or criminal past,[96] the basic First Amendment rule is that while the government may restrict conduct, it generally can't restrict speech simply because some people may at some time be moved by the speech to act illegally.[97] The law has plenty of tools to fight such discrimination directly. They are not perfect tools, but under the First Amendment the government may not try to compensate for their imperfection by suppressing speech.

The government may not suppress advocacy of discrimination based on race, criminal history, alcoholism, drug use, or pizza consumption, even though such advocacy may lead some people to actually engage in such discrimination. Likewise, the government may not suppress speech about particular people's criminal history, alcoholism, drug use, or pizza consumption, even though such speech may lead some people to engage in the discrimination.

2. *Fraud and violent crime.*

In a few cases, revealing certain information about people may make it easier for others to defraud or otherwise victimize them.

Under what circumstances the government may restrict speech that facilitates the commission of crime is a difficult and so far largely uninvestigated question.[98] It arises in many cases which have nothing to do with revelation of personal information, because personal information is just one of many kinds of information that can make it easier for people to commit crimes. For instance, the most prominent recent case that upheld a restriction on crime-facilitating speech involved a lawsuit against the publisher of a murder-for-hire manual.[99]

Moreover, even crime-facilitating speech that's focused on particular targets may involve information that few would consider especially private: For example, if we're concerned about speech that facilitates fraud or theft, publishing information about a business's security vulnerabilities or a list of the business's computer passwords may create as much risk of fraud as publishing a person's social security number would.

I won't try to resolve this question here, but only want to offer three observations. First, the fact that speech facilitates crime doesn't always justify restricting the speech (even if it sometimes might): Consider, for instance, normal chemistry books, which may be used by criminals to learn how to make explosives,[100] or detective stories that describe particularly effective ways to commit a crime.

Second, the strongest argument for restricting speech that reveals crime-facilitating personal information is that the speech facilitates crime, not that it reveals personal information. It is therefore probably most useful to analyze such speech as a kind of crime-facilitating speech, rather than as a specimen of revelation of personal data.

Third, the crime facilitation concern at most supports narrow restrictions on the particular kinds of speech that materially risk facilitating crime.[101] Whatever support there may be for a general right to suppress either speech that reveals embarrassing personal information or speech that reveals information about a person's purchases, the fact that a few kinds of such speech may facilitate crime can't justify these broad restrictions.

CONCLUSION

I have made three arguments:

---

[95] Employers not only have moral and business reasons to make sure that they don't hire people who might abuse their customers, but legal reasons, too: A negligent failure to discover that an employee has a criminal record may lead to liability for negligent hiring if the employee later attacks a customer. *See, e.g.,* Carlsen v. Wackenhut Corp., 868 P.2d 882, 888 (Wash. App. 1994).

[96] *See* N.Y. CORR. LAW §§ 752, 753 (generally barring employment discrimination based on criminal record); WISC. STAT. ANN. §§ 111.31, 111.32 (same).

[97] *See, e.g.,* Brandenburg v. Ohio, 395 U.S. 444 (1969).

[98] *See* U.S. Department of Justice, 1997 Report on the Availability of Bombmaking Information, available at <http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html>; KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE (1989); Eugene Volokh, *Crime-Facilitating Speech* (in progress).

[99] *See* Rice v. Paladin Press, 128 F.3d 233 (4th Cir. 1997).

[100] *See, e.g.,* U.S. Department of Justice, *supra* note 97 (listing a chemistry book from the respected Telford Press and books on explosives from the U.S. Bureau of Mines and the Association of Australian State Road Authorities among sources "useful to individuals bent upon constructing bombs and other dangerous weapons").

[101] *Cf.* Florida Star v. B.J.F., 491 U.S. 524, 537, 539 (1989); *id.* at 542 (Scalia, J., concurring in part and concurring in the judgment).

1. Despite their intuitive appeal, restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied. There might possibly be room for restrictions on revelations that are both extremely embarrassing and seem to have virtually no redeeming value, such as unauthorized distribution of nude pictures or possibly the publication of the names of rape victims, and perhaps for speech that makes it substantially easier for people to commit crimes against its subjects. Even these, though, pose significant doctrinal problems.

2. Asking courts to expand the doctrine to create a new exception may give supporters of information privacy speech restrictions much more than they bargained for. All the proposals for such expansion—whether based on an intellectual property theory, a commercial speech theory, a private concern speech theory, or a compelling government interest theory—would, if accepted, become strong precedent for other speech restrictions, including ones that have already been proposed. The analogies between the arguments used to support information privacy speech restrictions and the arguments used to support the other restrictions are direct and powerful.

And accepting the principles that the government should enforce a right to stop others from speaking about us and that it's the government's job to create "codes of fair information practices" controlling private parties' speech may shift courts and the public to an attitude that is more accepting of government policing of speech generally. The risk of unintended consequences thus seems to me quite high.

3. People who generally oppose any broad diminution of free speech protections but who think information privacy speech restrictions must be upheld, can try to set forth their proposed new exception and its supporting arguments as carefully and narrowly as possible. I hope their attempt to craft such a well-cabined, narrow rationale for any such new exception will be helped by this Article, which highlights some of the analogies that generally pro-speech-restriction forces might use to expand any exception that is created. Maybe with a very carefully drawn exception, my fears about the unintended consequences of recognizing such exceptions won't come to pass.

But some people may reluctantly conclude that the risk is just too great. We protect a good deal of speech we hate because we fear that restricting it will jeopardize the speech we value. Some people may likewise conclude that it's better to protect information privacy in ways other than speech restriction—through contract, technological self-protection, market pressures, restraints on government collection and revelation of information, and social norms—than to create a new exception that may eventually justify many more restrictions than the one for which it is created.

Mr. STEARNS. Professor Rubin?

STATEMENT OF PAUL RUBIN

Mr. RUBIN. Thank you, Mr. Chairman and members of the subcommittee. I thank you for letting me testify.

Mr. STEARNS. Could you just pull one of the microphones up to you?

Mr. RUBIN. Oh, I am sorry.

Mr. STEARNS. That is fine.

Mr. RUBIN. Thank you for inviting me to testify today.

Mr. STEARNS. Maybe just a shade closer. Good.

Mr. RUBIN. I am currently in the process of completing a major study of the issue of privacy for the Progress and Freedom Foundation. My testimony and the forthcoming study is concerned with the commercial market for personal information that is used for advertising and marketing purposes, so I want to confine my remarks to that segment of the issue.

In my written testimony, I make five basic points. First, consumers receive large benefits from the commercial use of information. Advertising revenues support many valuable services that are provided free over the Internet, and we all know what some of these are. Information makes it possible to target advertising messages to consumers' interests, and the result is, as Professor Cate indicated, better information; reduces the amount of spam and

other undesired messages, because advertisers are better able to target us if they have this information.

Second, the way information is used on the Internet is highly impersonal. Humans do not see or handle the information. It is generated and manipulated by computers. So we have this intuition that somebody knows something, but in many cases, the knowledge is embedded on a computer somewhere; no person has access to the information. The typical unit of commerce in online advertising is an ad based on 1,000 browsers. So it is a large block of potential viewers rather than an individual.

Third point: despite consumer concerns, there does not appear to be actual evidence of harm to consumers from the legal use of information for marketing and advertising purposes. I want to stress that it is the legal information, so there are illegal uses, of course, but the legal use does not seem to have led to any harm. We have heard some stories from members of the committee this morning on, for example, medical records and so forth, but these are not commercial use of information. From the commercial use, there seems to be no evidence.

In a year-end summary dealing with privacy issues, C-NET, a leading new economy news source, said despite the fears and concerns, there were no publicized horror stories that resulted from a privacy invasion. As I said, illegal use of information such as credit card fraud and identity theft do cause real harms. These are already, of course, against the law and do not appear to be closely related to online activities. James Hust, the Inspector General of the U.S. said with respect to identity theft this is not an Internet crime and never was, and the FTC is on record—officials of the FTC are on record also indicating that there is no higher level, no evidence of a higher level of fraud or identity theft based on the Internet than based on other sources of information.

The fourth point: we have heard people say that privacy is good business, and I think it is good business, and what you expect if something is good business, you expect business to respond, and we have a lot of evidence that business is, in fact, responding to privacy concerns. I have some charts here. The first chart indicates that in several cases, firms have undertaken some action which has later turned out to bother consumers; consumers protested, and the firms have canceled the action solely based on consumer response. Probably the best-known is Double-Click's purchase of Abacus, which was canceled because of consumer concerns about the use of information.

So there is a mechanism there. Second, there are voluntary standards organizations, numerous voluntary standards organizations; trustee; BBB Online; the Direct Marketing Association has principles of privacy; and accounting firms provide privacy audits; again, a market response to privacy issues. There is also something about to come online, P3P, which has been mentioned and may go a long way toward alleviating privacy concerns.

And then, we see firms beginning to advertise privacy as well. Part of this morning's Post has an article: Earthlink resorts to restroom ads, but the restroom ads referred to in the Post deal with privacy. So firms are perceiving that privacy is something consumers want, and not only are they posting privacy policies on

their Websites, but they are actually advertising that they offer better privacy.

Fourth, there are lots of technologies that consumers can use: cookie rejection technologies, anonymous browsers, so there are alternatives out there for consumers particularly concerned with privacy.

The fifth point: regulation of the market for personal information is potentially very costly. Congress should proceed cautiously based on a careful evaluation of the benefits and costs. Based on the evidence thusfar available, the case for new regulation is weak. The market seems to be rapidly evolving to meet privacy concerns. Regulation of the market would entail cost in terms of fewer consumer choices. It would also have an adverse effect on innovation and competition. These costs are likely to outweigh potential benefits which appear small, because there is little evidence that consumers are now being harmed by misuse of this information.

Thank you.

[The prepared statement of Paul Rubin follows:]

PREPARED STATEMENT OF PAUL H. RUBIN,[1] PROFESSOR OF ECONOMICS AND LAW, EMORY UNIVERSITY

Mr. Chairman and Members of the Subcommittee: I appreciate the opportunity to testify on "Privacy in the Commercial World." I am currently in the process of completing a major study of this issue for The Progress & Freedom Foundation.

Recent advances in information technologies have reduced the costs of collecting, storing, retrieving and transmitting information of all kinds. While the economic and social impacts of these advances have been overwhelmingly positive, they have also raised concerns on the part of individuals about who has access to their personal information and how it is being used. These concerns, in turn, have led to calls for new government regulation.

In order to decide whether regulation is in order, and, if so, what form it should take, basic public policy questions need to be answered:

- Are there market failures in the market for personal information?
- If market failures exist, how do they adversely affect consumers?
- Can such failures be remedied by government regulation?
- Would the benefits of government regulation exceed the costs?
- Are specific legislative and/or regulatory proposals cost-effective in achieving their goals.

The purpose of the PFF study is to make a start toward answering these questions.

My testimony—and the forthcoming PFF study—is concerned with the commercial market for personal information that is used for advertising and marketing purposes. Thus, it does not specifically address a number of other issues that are sometimes discussed under the overall umbrella of "privacy," but raise different concerns.

My work does not address particularly sensitive types of information, such as health information, personal financial information or information about children. These types of information are already subject to regulatory programs specifically tailored for them.

I also do not address illegal uses of information, such as credit card fraud and identity theft. These are serious crimes, and impose significant costs on consumers and businesses. However, they are already against the law. Identity theft is a Federal crime, and a crime in 22 states,[2] and the use of someone else's credit card is illegal in all 50 states.

Moreover, the incidence of these crimes does not appear to be related to online activities. In a recent article, for example, Betsy Broder, Assistant Director for Planning and Information at the FTC is quoted as saying: "The Internet is probably not

---

[1] Paul Rubin is Professor of Economics and Law at Emory University and Senior Fellow at The Progress & Freedom Foundation. The views expressed here are his own.

[2] CALPIRG, "Nowhere to Turn: Victims Speak Out On Identity Theft," available on the CALPIRG Website, http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/toppage1.htm visited January 12, 2001.

as large a part of the problem [of identity theft] as people suspect."[3] Ms. Broder also said "None of the statistics show a greater vulnerability of consumers who are shopping online."[4] This is consistent with the findings of a study of 66 victims of identity theft, which found that only two of the 66 (about three percent) "had reason to believe that the thief had obtained their information via the Internet."[5] The Inspector General of the United States, James Huse, has said, with respect to identity theft, "This is not an Internet crime and never was."[6]

Finally, my testimony does not concern government collection and use of information. Because, as a nation, we are concerned about the misuse of government power, government is constitutionally constrained in its ability to obtain information about individuals, as when it uses software such as "Carnivore" to search emails. It is also justifiable to hold government to a stricter standard with respect to the information it controls, because government has mandatory access to much of that information.

THE COMMERCIAL USE OF PERSONAL INFORMATION

Data on individuals has been used by marketers and advertisers long before the advent of the Internet. But, the Internet has increased the flow of personal information and, in the process, raised the level of individuals' concerns about privacy.

On the Internet, targeted advertising is accomplished by examining individuals' online activities, developing an understanding of their interests, and then matching and delivering relevant advertisements. This is accomplished by compiling individuals' web-browsing activities and applying database technologies and statistical models that yield demographic and interest profiles, commonly referred to as consumer profiles. Advertisements relevant to consumers' profiles are then inserted in the Web pages they visit.

Advertising firms, such as DoubleClick and 24/7, deliver targeted advertisements to Internet users that visit popular Websites. Website operators receive advertising revenues based on pages viewed and advertisements delivered. Advertising is a major source of revenue for Websites such as search engines, directories and portals, and is growing rapidly. U.S. companies spent $3.5 billion on Web advertising in 1999. Revenue in the second quarter of 2000 was $2.1 billion. Advertising spending on the Web is predicted to increase to $16.5 billion by 2005, making online spending eight percent of the total amount spent on advertising.[7] This advertising in turn fuels billions of dollars in online purchases.

Advertisers use personal data to identify individuals who are more interested than the average in purchasing some product or service. The search begins with the product, and seeks out individuals who might have an interest in the product. A seller does not ask "What can I sell to Paul Rubin?" Rather, a seller asks an advertiser such as DoubleClick or 24/7 to "Put my ad on 1,000,000 pages viewed on computers of persons more likely than average to want a new car" and perhaps Paul Rubin's computer turns out to be one of those selected. But, no human makes this determination; rather, it is made by various computers connecting with each other. Moreover, the unit of commerce in the online advertising market is typically 1000 persons, not any individual.[8]

CONSUMER BENEFITS

Consumers benefit from this advertising in numerous ways. First, advertising revenues support many valuable services that are provided to consumers at no charge. These services include free email and pages from firms like Yahoo! customized to contain information of direct interest to the particular individual.[9] The amount of

---

[3] Quoted in Danielle Sessa, "The Best Way to . . . Keep Safe," *The Wall Street Journal,* Nov. 27, 2000, R25.

[4] Quoted in Susan Stellin, "Using Credit Cards Online Remains Safe Despite High-Profile Security Lapses," *New York Times* October 16, 2000.

[5] CALPIRG, "Nowhere to Turn: Victims Speak Out On Identity Theft," available on the CALPIRG Website, http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/toppage1.htm visited January 12, 2001, p. 6.

[6] Scott Bernard Nelson, "Identity Crisis," *The Boston Globe,* August 27, 2000. He does add: "But technology has created new ways of storing and selling personal information and it's likely to create more and more headaches in the future."

[7] The Standard, "Net Ads Keep on Ticking," by Stacey Lawrence, September 4, 2000. Available on-line at: http://www.thestandard.com/research/metrics/display/0,2799,18155,00.html. Visited September 20, 2000.

[8] "All rates are expressed in cost per thousand (CPM) ad banner impressions." From DoubleClick's Rate Card, http://www.doubleclick.net:80/us/advertisers/media/network/info/ratecard.asp?asp__object__1=& , visited February 22, 2001.

[9] I use a free customized page from Yahoo! as my own homepage. This contains information in many categories that I have selected: headlines on selected topics from Reuters and AP; infor-

free information available on the Internet is truly remarkable, and this information is paid for through advertising. Internet advertising firms such as DoubleClick provide customized advertising to smaller Websites that use the revenues from this advertising to support themselves. Larger firms, such as AOL and Yahoo!, can internally provide the same services that DoubleClick and its competitors provide for the smaller sites.

Second, consumers benefit from receiving information that is targeted to their interests. Consumers value learning about products they are likely to buy. Even if some advertising does not lead directly to a purchase, the information may still enable a consumer to compare prices among products, or to determine what products are available.

Targeted advertising reduces the likelihood that consumers will be bothered with information that is of no interest to them, and marketers have an incentive to avoid sending messages to consumers who aren't interested. Consumers are likely to avoid Websites that routinely display useless information, or to ignore, delete or screen out messages from marketers who send the irrelevant emails commonly described as "spam." Thus, both consumers and advertisers have an interest in better targeting of advertising messages.

Generally, markets work better with better information. As the cost of information goes down, market participants will obtain more of it and will consequently make better decisions. For example, if merchants can better estimate demand, they are less likely to purchase excess inventories, reducing costs and even lessening swings in overall economic activity. Similarly, geographic computer-based information can enable bricks-and-mortar merchants to put their new stores in the places that best serve consumers, and to stock the most useful merchandise for nearby consumers in those stores. Such examples can be multiplied without limit—all agents in the economy will benefit from better information. Electronic information has led to a major reduction in the cost of information and therefore a major increase in the amount of information available to the economy, and any policy that reduces the amount of such information below the efficient amount will have detrimental effects on the economy.

Finally, an important characteristic of information is that—in contrast to many other goods—it can be used many times without being used up. If I know something and tell you, then we both know it. This "public good" characteristic is an important reason for the productivity of information. For the type of commercial information discussed here, advertisers, credit institutions, and insurance companies use the same information, and it is useful to all of them. Indeed, the various information users cooperate in generating this information because they all find it valuable.

Thus, if there are externalities associated with the commercial use of information, they are more likely to be positive than negative. This means that it is more likely that not enough information is available than that too much information is available. Regulation that would reduce the use and availability of information would exacerbate this problem.[10]

IS THERE MARKET FAILURE?

From an economic point of view, regulation of the market for information should only be undertaken if the market is not functioning correctly. Market failure in this context would mean that consumers' preferences concerning the amount and use of their information are not being accurately transmitted and responded to in the marketplace. If the market is working well, there is no need for government intervention.

Consumer Harm

Given widespread consumer concerns about privacy and perceptions that personal information may be subject to misuse, it is noteworthy that there does not appear to be actual evidence of harm to consumers from the legal use of information for marketing and advertising purposes. In an economy with 281 million individuals, there does not even appear to be much in the way of anecdotal evidence of harms resulting from violations of privacy in connection with such marketing activities. For example, in a year-end summary for 2000 dealing with privacy issues, CNET, a

---

mation about chosen stocks and stock indices; weather in selected cities; and movies in my neighborhood. Many other categories are also available. For all of this information, much more detail is available from a mouseclick.

[10] It is sometimes argued that information should be used only for the purpose for which was collected. In fact, this is part of the European Union Directive on the Protection of it Personal Data. However, this restriction on information use imposes a real cost on the economy, in that many productive uses would be denied.

leading "New Economy" news source, indicated that there were no mishaps involving commercial use of personal information in 2000: "Despite the fears and concerns, there were no publicized horror stories that resulted from a privacy invasion." [11]

Much of the anecdotal evidence of "harm" that does exist concerns activities that have nothing to do with the use of information for marketing purposes. For example, a *New York Times* magazine article by Jeffrey Rosen [12] provides anecdotes about individuals who have been harmed by invasions of their privacy, but none concern misuse of advertising data. He discusses, for example, Monica Lewinsky's emails and various archives kept by chat rooms, and employer monitoring of email and surfing. None of his evidence or examples of harm apply to marketing or advertising information.

It might be argued that, even though there has been no harm thus far, there might be in the future. But, given the absence of harm thus far, the risk would seem to be small.

Consumer Interaction with Websites

Perhaps part of the reason we see no evidence of consumer harm is that there are a variety of market mechanisms now available to consumers to make known their preferences with respect to the use of their personal information.

Reputation Effects. Consumers are not without recourse if firms use their information in ways they don't like. Consumers can simply stop doing business with the offending firm, and the evidence shows they are quite willing to do so. In fact, reputation effects are powerful, and the evidence shows that when a firm does something that is perceived as harming its reputation with consumers, the firm suffers a substantial loss in value.[13]

Reputation effects can be expected to be particularly strong among firms operating on the Internet, where communication between consumers is easy and inexpensive. Consumers quickly learn about what they perceive as misdeeds by a firm:

- When Amazon appeared to have engaged in "dynamic pricing" (what economists call price discrimination) consumers learned about it quickly and many became irate.[14] Such pricing is probably efficient, [15] but nonetheless the firm has promised not to engage in this practice.
- In 1997, America Online had plans to sell telephone numbers of its subscribers to telemarketers, but cancelled those plans in response to angry reactions from subscribers.[16]
- In 1998, CVS pharmacy arranged for another company to contact consumers who failed to refill prescriptions. Again, consumer dissatisfaction led to the plans being called off.
- In 1999, RealNetworks was forced to change its software when it was learned that its product, RealJukebox, collected information on users' habits.
- Yahoo! eliminated the reverse telephone number search from its search site in response to consumer unhappiness.[17]
- Lotus cancelled plans to sell data about 120 million citizens.
- Lexis-Nexis also cancelled plans to sell information about millions of persons.
- More recently, a firm called N2H2, which makes filtering software, has stopped selling information about Websites visited by students, because many felt that such sales were improper.[18]

---

[11] Patricia Jacobus, "Privacy heats up but doesn't boil over," CNET News, December 22, 2000, available online at http://news.cnet.com/news/0-1005-200-4238135.html?tag=st.cn.sr.ne.1, visited December 25, 2000.

[12] Jeffrey Rosen (2000), "The Eroded Self," *New York Times Magazine,* April 30, p. 46.

[13] For a summary of the literature, see Kari Jones and Paul H. Rubin, "Effects of Harmful Environmental Events on the Reputations of Firms," *Advances in Financial Economics* (forthcoming), 2001, edited by Mark Hirschey, Kose John and Anil K Makhija, available online at http://papers.ssrn.com/paper.taf?ABSTRACT_ID=158849.

[14] David Streitfeld, "On the Web, Price Tags Blur," *Washington Post,* September 27, 2000. Amazon denies that it was engaged in dynamic pricing or price discrimination.

[15] Paul Krugman (2000), "What Price Fairness?", *New York Times* October 4.

[16] This and the following two examples are from Jessica Litman, "Information Privacy/Information Property," 52 *Stanford Law Review,* 1283-1313, May, 2000, at 1305-6.

[17] This and the following two examples are from Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," p. 27, available online through SSRN.Com, 56-57.

[18] Associated Press, "Internet Co. Drops Data Selling Plan," Feb. 22, 2001. Note that the plan did not sell personally identifiable information.

- Finally, there is the well-known story of DoubleClick's cancelled plan to link on-line and personally identifiable information through its acquisition of Abacus Direct.[19]

The critical point is that when businesses use information in ways that consumers do not like, they quickly learn about it, and the firms are forced to stop. Such reputational penalties may be among the strongest protections available to consumers. The main asset that on-line marketers own is their reputation with consumers. Any use of information in a way that reduces the value of that reputation would be counterproductive for the firm. Moreover, the very nature of information on the Internet means that consumers are likely to learn about such uses.

This suggests that arguments about asymmetric information, such as have been advanced by Peter Swire, are incorrect.[20] Such arguments claim that consumers will not have adequate incentives to learn about the policies of any Website with respect to privacy, and therefore Websites will not have adequate incentives to provide appropriate privacy protections. This may be true for many consumers. However, as discussed above, if they find privacy policies unsatisfactory, when they do learn about them, the market reaction will be strongly adverse. This provides a sufficient incentive to Websites to provide their customers with satisfactory privacy policies.

We also see firms taking many positive steps to protect their reputations. IBM, Microsoft, Disney, Intel, Compaq, Novell, Procter & Gamble, and American Express do not advertise on Websites that do not have privacy policies.[21] Presumably, this is to protect their reputations. As a method of protecting reputations, firms are increasingly hiring "chief privacy officers" (CPOs) and giving them substantial power and discretion in setting company policies. Alan Westin, a well-known privacy expert, offers a training course for this position.[22] There are now about 100 CPOs, and it is estimated that there will be 500 by the end of next year.[23]

Technologies of Choice. There are numerous technologies now available that allow consumers to address their privacy concerns:

- Basic browsers now allow some customization with little effort. For example, Netscape allows a user four options with respect to cookies. Microsoft also offers some control.
- Other options allow control of cookies. From one site, approximately forty programs that allow control of cookies can be downloaded.[24] These programs allow one to refuse certain cookies, or to easily delete cookies after they are received.
- There are also several services that allow anonymous surfing, including Anonymizer.com, IDZap.Com, iPrivacy.com, SafeWeb, SilentSurf.com, and others as well. These services offer different levels of control over information, depending on the consumer's preferences and willingness to bear the inconvenience costs of protecting information.
- In addition, American Express now offers a "one-time" credit card number, good only for one purchase, designed for Internet use. Since Websites selling products to consumers using this card never have access to information about the consumer, privacy is protected.

Consumers concerned about privacy are able to use any of these services, some free, to protect their information online.[25]

Importantly, the World Wide Web Consortium (W3C), a consortium of 488 members (as of December 22, 2000), including the largest players on the Internet, such as Microsoft, America Online and Cisco,[26] is in the process of drafting a major pri-

---

[19] Discussed at numerous places. See for example Diane Anderson and Keith Perine, "Marketing the Double Click Way," *The Standard,* March 13, 2000.

[20] See Peter Swire, "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in Privacy and Self-Regulation in the Information Age, U. S. Department of Commerce, Washington, DC, 1997, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm.

[21] "It's Time for Rules in Wonderland," *Business Week,* March 20, 2000; "Towards Digital eQuality—The Second Annual Report of the US Government's Work Group On Electronic Commerce", December, 1999.

[22] http://www.pandab.org/.,visited November 13, 2000.

[23] Kemba J. Dunham, "The Jungle: Focus on Recruitment, Pay and Getting Ahead: A New Playing Field," *The Wall Street Journal* March 20, 2001.

[24] Downloaded on October 25, 2000 from ZDNet Downloads (http://www.zdnet.com/downloads/), a popular source for software, using a search for "cookie"

[25] Some of these are discussed in Don Clark, "Privacy: You Have No Secrets," *The Wall Street Journal,* October 23, 2000 and Lorrie Faith Cranor, "Agents of Choice: Tools That Facilitate Notice and Choice about Web Site Data Practices", available online from http://www.research.att.com/~lorrie/#publications.

[26] For the W3C homepage, see http://www.w3.org. For the list of members, see http://www.w3.org/Consortium/Member/List, visited December 22, 2000.

vate privacy protocol, the Privacy Preferences Project, P3P.[27] If P3P is successful, it will provide standardized information in machine-readable form about each Website's privacy policy. Individuals will then be able to configure their own browsers to deal with the Website. Major players in the Internet world are participants in this endeavor. Moreover, Microsoft will begin incorporating P3P standards in its software.[28] It will also be available as a downloadable plug-in.[29] This will solve one side of the "chicken-and-egg" problem. Since the software will be available to consumers, Websites will have a ready-made audience if they install the other side of the package. Lessig[30] also discusses the possibility of P3P leading to increased negotiation and customization of privacy policies, as do several others.

There are other technologies on the horizon that may provide other solutions. One is the evolution of "trusted systems." These are envisioned as computer protections that limit the way in which data can be copied. While they are being developed to protect intellectual property, such as music, movies and books, it may be possible for these technologies to be adapted to protect consumer information as well.[31]

Voluntary Standards. Voluntary standards, defined and enforced by third parties or by consortia of Web operators, are an important mechanism to inform consumers that a Website meets certain minimum standards. Such standards improve the functioning of the market and are not merely an attempt by industry to ward off government regulation.

There are already several voluntary programs in existence that certify that a Website meets certain privacy standards:

- A Website can voluntarily join TRUSTe, for example. [32] If it does, a link is put on the website and by clicking on this link, a visitor can view the site's privacy policy. TRUSTe audits Websites to ensure compliance with stated privacy policies. As of December 22, 2000, 1,570 firms were members of TRUSTe.[33]
- The Better Business Bureau also has a certifying program, BBBOnLine, that performs similar functions.[34]
- The Direct Marketing Association has various voluntary standards in place, including a method consumers can use to have their names removed from email lists, and members of the association must meet certain requirements regarding privacy on the Web.[35]
- Finally, auditing firms, such as PriceWaterhouseCoopers, perform privacy audits and put a box on a website indicating that the site conforms with its stated privacy policy.[36]

There is evidence that voluntary standards in the U.S. actually work better than mandatory standards imposed by the European Commission.[37] For example, although "opt-out" is required in Europe, only 20 percent of Websites actually offer this option to consumers; in the U.S., 60 percent of sites offer this choice. About twice as many U.S. sites (62 percent) as European sites (32 percent) have posted privacy policies. Although all members of the EU now have data-privacy commissioners and agencies, these agencies seem unable to enforce privacy regulations. Thus, it appears that voluntary self-regulation provides more privacy protection than does mandatory government-imposed regulation.

THE BENEFITS AND COSTS OF REGULATION

The discussion above suggests that the market is responding well to consumers privacy concerns. Firms have incentives to provide consumers the desired levels of privacy protection and consumers have tools available to inform themselves about, and control the use of, their data. In addition, there seems to be little if any evidence that consumers are suffering harm from the commercial use (or misuse) of their personal information. While every regulatory proposal should be subjected to

---

[27] http://www.w3.org/P3P/.

[28] "New Tools to Help Web Surfers Protect Privacy," Associated Press, June 22, 2000.

[29] Elizabeth Weise, "Privacy plug-in will ask: 'Do you want to go there?'" USA Today, July 11, 2000.

[30] Lawrence Lessig, "The Architecture of Privacy," 1998, Online, http://cyber.law.harvard.edu/works/lessig/architecture__priv.pdf.

[31] Jonathan Zittrain, "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, 52 *Stanford Law Review* 1201-1250, May 2000.

[32] Website: http://www.truste.org.

[33] Found at http://www.truste.org/users/users__lookup.html visited December 22, 2000.

[34] http://www.bbbonline.org/

[35] http://www.the-dma.org.

[36] Bob Tedeschi "Sellers Hire Auditors to Verify Privacy Policies and Increase Trust," New York Times, September 18, 2000.

[37] Ben Vickers, "Europe Lags Behind U.S. on Web Privacy: More American Firms Let Customers Guard Data, Study Finds," *The Wall Street Journal,* February 20, 2001.

a detailed benefit-cost analysis, the absence of serious market failure or consumer harm suggests that the potential benefits of new regulation will be very small.

The costs, on the other hand, can be significant, because regulation is a cumbersome, inflexible tool and because we do not now have the knowledge base to regulate intelligently in this area. As I discuss below, regulation can have adverse effects on both innovation and competition and slow the development of the Internet economy.

It is a cliché to say that the Internet is dynamic. But, it is true. Any regulation at this time would freeze some aspects of the Internet in their current state. Even if the regulators were able to devise perfect regulations for today's environment, these regulations would quickly become obsolete as the Internet changes. The P3P release is P3P 1.0, indicating that, like software in general, the drafters expect that the privacy policies embedded in the document will change over time. Indeed, at several places in the document itself there are indications of directions for change in future versions. Change is the normal state of affairs for the Internet and for software and other products that interact with the Internet.

Once an inefficient regulatory scheme is in place, however, it becomes very difficult to change. This suggests moving with great caution in this area. The FTC has recommended that Congress pass a law regulating four aspects of privacy: Notice, Choice, Access and Security.[38] These may be the correct elements for a privacy policy to address. But they also may not be, and the FTC has not done the analysis necessary to show that they are. If it should turn out that other policies are better, the Internet would nonetheless be locked into the FTC's choices. The FTC's desire that all Websites structure their privacy policy in the terms dictated by the FTC would have the effect of freezing in place a particular policy. This policy may not be the best policy now, and almost certainly will not be the best policy for the future.

Effect on Choice

Regulation of this sort is of necessity the "one size fits all" variety. This might be justified if all consumers had similar or identical preferences. But, it is difficult to justify what are in essence mandatory product design regulations if preferences differ substantially, as is the case with respect to privacy. Some consumers view privacy protection as a good thing, but others welcome the advertising information they receive when they give out information about themselves. As an industry source puts it, "What's an invasion of privacy to one consumer is a great deal to another."[39] When preferences do differ in such significant ways, then some consumers must be harmed by regulation.

With respect to Internet privacy, the FTC itself acknowledges that consumers differ in their privacy preferences: "According to one panelist, survey research consistently indicates that roughly one-quarter of the American public is "intensely" concerned about privacy and that another quarter has little or no concern; the remaining fifty percent view this issue pragmatically."[40] These differences are documented carefully in a survey on Internet privacy by AT&T.[41] For example, those most concerned about Internet privacy—those the AT&T report calls "privacy fundamentalists"—can already protect themselves using a variety of techniques discussed above. On the other hand, some consumers are so little concerned with privacy issues that they are willing to have all of their Web surfing monitored. AllAdvantage.com pays consumers to monitor their browsing, and some consumers (presumably those less concerned with privacy issues) are apparently willing to join this program.[42] Dash.com provides discounts to consumers who allow monitoring. Many other companies provide discounts and benefits of various kinds to consumers who are willing to share their information. Thus, consumers have radically different preferences regarding Internet privacy, and markets are now satisfying all types of preferences. Privacy regulations could have the effect of making some business plans infeasible and thereby depriving consumers of goods and services that are now available.

---

[38] Federal Trade Commission (2000), *Privacy Online: Fair Information Practices in the Electronic Marketplace,* May 2000. For comments on the FTC's proposal, see Orson Swindle, "Privacy in a Digital World: Industry Must Lead, or Government Will Follow," The Progress & Freedom Foundation, March 2001 (attached).

[39] Margaret Barnett, The Profilers: Invisible Friends, *The Industry Standard,* March 13, 2000, p. 221.

[40] In its 1998 Report, Part II, at 2.

[41] Lorrie Faith Cranor, Joesph Reagle, and Mark S. Ackerman, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," AT&T Labs-Research Technical Report TR 99.4.3, 1999http://www.research.att.com/library/trs/TRs/99/99.4/

[42] http://www.alladvantage.com/home.asp?refid=

The AT&T Report also finds that consumers have very different privacy preferences regarding different types of information. For example, consumers are less willing to provide Social Security and credit card numbers than other types of information. Similarly, 78 percent would accept cookies to provide a customized service; 60 percent would accept a cookie for customized advertising; and 44 percent would accept cookies that convey information to many Web sites. This means that any standardized privacy notice would have to be exceedingly complex—so complex that few people would be willing to read it. Moreover, different pages within the same site might require different policies, so virtually each mouse click would require reading a new notice. On the other hand, a protocol such as P3P could provide customized settings for each type of information and each potential use, based on consumers filling out a one-time form when configuring their browsers. Of course, some consumers would choose not to do so and would merely accept the defaults.

Effect on Innovation

Regulation will affect potential new uses of the Internet. Uses that might otherwise develop will be hindered by excessive regulation. The costs in terms of lost innovation are difficult, if not impossible, to quantify, because we are not likely to know about potential new uses that do not come into being because of regulation. Nonetheless, these costs are real, and probably larger than the measurable, direct costs of regulation.

For example, the Internet is becoming more available on handheld units, also called Personal Digital Assistants (PDAs), and on Web-enabled cell phones. Technologies for such uses are becoming increasingly easy to use. Some are wireless: Websites are broadcast to users. Additionally, it is possible to download Websites to handhelds in the process of synchronizing the PDA with a desktop computer. There are even new technologies that may make Web information available through audio means. But the interaction of these new technologies with privacy policies is problematic. One difficulty is provision of notification policies on a PDA or mobile telephone screen; these screens are too small and too slow to display meaningful notice information. Having notice policies read aloud by an audio-enabled Website would be even more impractical.

Moreover, it is commonly agreed that a major innovation in the use of the Internet is the increasing extent to which it will be possible to track the geographic location of individual consumers, using mobile phones or PDAs with GPS chips.[43] One advantage of the technology (and one of its sources) is a desire by the government to better deliver emergency services to injured persons. Chips in mobile telephones and other devices and PDAs will have tracking abilities. The chips will enable individuals to obtain personalized information relevant to their location, such as driving directions or the location of restaurants or movies. General Motors is planning to use this technology to send information to users of its OnStar vehicle-based navigation system.[44] Privacy issues are important with these devices. Palm is developing an opt-in program for location chips. DoubleClick will not begin delivering ads until privacy issues are worked out. TRUSTe is developing standards for privacy policies. Of course, the difficulties with presenting privacy policies on small screens applies to these uses as well.

There are at least two lessons from the story of this technology. First, industry is already responding to privacy concerns in developing this technology, because it is responding to consumer preferences. Second, if a government-mandated privacy policy were in place, it could retard or even entirely stop the development of these technologies. For example, if there were a law mandating notice and standards for notice, the requirements could be inconsistent with the size of screen available, and certainly with audible websites. If this were so, then consumers could lose the benefits of a valuable technology. This potential loss, should it occur, would not even be recognized; people do not miss technologies that do not exist.

Effect on Competition

Regulation of privacy has competitive implications as well. More stringent regulatory requirements would have the effect of reducing advertising, which typically benefits new entrants and small firms relative to large, established firms.[45] This would be particularly true for Internet advertising, where established firms have lists of their own customers and visitors to their Websites, but new firms must pur-

---

[43] Discussed, for example, in Anick Jesdanun, "Wireless Tracking Device Coming Soon," AP, October 29, 2000 and Pui-Wing Tam, "...Know Where We Are," *Wall Street Journal,* November 13, 2000.

[44] Rachel Konrad, General Motors to 'push' ads to drivers," CNET News.com, January 8, 2001.

[45] John E. Calfee, *Fear of Persuasion: A New Perspective on Advertising and Regulation,* American Enterprise Institute, Washington, 1997.

chase such lists. The existence of a market for customer lists and other such information makes it easier for entrants to begin competing. If regulation should reduce the scope of this market or increase the cost of information, then competition from new entrants would be reduced.

New privacy standards would also make entry more difficult by increasing the fixed costs of doing business. Every online marketer would be required to hire an attorney at least to write a "notice" about privacy policies; full-time CPOs earn between $120,000 and $175,000 per year.[46] Allowing access and enforcing security would also be costly. All of these costs are "fixed" costs, and so are higher per unit of output for small than for large firms. Thus, any such regulations would serve at least in part as a barrier to entry against small firms, and as a source of protection for large established firms. These policies would lead to increased prices and reduced service and, thus, harm consumers.

In the Internet economy, small startup companies with new ideas and new business models have been a particularly important source of innovation. Regulations mandating privacy policies or other regulations are particularly likely to be harmful in this environment.[47]

CONCLUSION

To summarize, regulation of the market for personal information should proceed cautiously, based on a careful evaluation of the benefits and costs of any specific regulatory proposal. Based on the evidence thus far available, the case for new regulation is weak. The market seems to be rapidly evolving to meet consumers' privacy concerns. Innovative new ways to address these concerns are rapidly becoming available.

Regulation of the market for personal information would entail costs in terms of fewer consumer choices. It would also have an adverse effect on innovation and competition. These costs are likely to outweigh the potential benefits, which appear to be small, because there is little evidence that consumers are now being harmed by misuse of marketing and advertising information.

Mr. STEARNS. Ms. Singleton?

STATEMENT OF SOLVEIG SINGLETON

Ms. SINGLETON. Thank you, Mr. Chairman, for this opportunity to offer a historical perspective on the law of privacy. I will try to do this in 5 minutes, which should be interesting.

My remarks mainly pertain to broad privacy laws that are not targeted at sectors where there are special contractual and sort of professional issues like medicine or to specific real harms like identity theft. My remarks are, rather, relevant to sort of broad privacy legislation affecting businesses across the board.

Let me begin my summing up what we can learn from privacy in the Nineteenth Century. There's essentially two aspects to Nineteenth Century privacy cases. There's some limited case law involving the private sector, and there's also, of course, Constitutional cases involving the Fourth Amendment.

Let me start with the private sector. There was a sort of nascent common law of privacy in the private sector at that time. For example, privacy was often recognized as an element in disputes over physical property rights such as easements and nuisances and that sort of thing. There was a lot of building going on in America during that time, and so, frequently, privacy questions would come up when two buildings were built very close together.

Now, the bit here that is relevant to today's debate about privacy is that when you see these privacy cases that essentially identify

[46] Kemba J. Dunham, "The Jungle: Focus on Recruitment, Pay and Getting Ahead: A New Playing Field," *The Wall Street Journal* March 20, 2001.

[47] Discussed in Peter P. Swire and Robert E. Litan (1998), *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive,* Washington: Brookings Institution Press, at 78-79.

privacy with physical property rights, there is no First Amendment problem. And that is because the property often helps us find boundaries of free speech, too. For example, you have a right to read books, obviously, but you can't go and steal books out of your neighbor's house or any other kind of information. So in that respect, privacy and First Amendment are quite consistent with one another.

Now, I am going to change tracks a little bit and talk about some of the privacy cases in the Constitution from the Nineteenth Century. Sometimes, in the debate about privacy and business today, one hears the assertion that privacy rights in the Constitution show that government has a strong interest in regulating privacy in the commercial sector. But actually, Constitutional privacy cases are rarely very relevant to the debate about privacy in business.

In the Nineteenth Century, and this continues today, courts do not apply the Fourth Amendment to the private sector, and essentially, the Fourth Amendment should not be a basis for asserting privacy rights against either journalists or commercial businesses where there is no State action, and the private sector enjoys Constitutional rights of free speech. Obviously, the police don't have a kind of Constitutional right to free speech to come into your home and search your things without a warrant. So again, on that traditional understanding of the Fourth Amendment, there is no conflict with free speech.

Now, I will jump ahead to privacy in the early Twentieth Century, which is where you first begin to see a tension between privacy and the First Amendment. Beginning in the early Twentieth Century, courts began to accept a concept of privacy that was detached from physical property rights a little bit akin to defamation or intellectual property but more expansive.

Now, over the years, many of those privacy torts were applied against journalists, and so, for the first time, we see serious free speech and privacy issues. And over the years, some of the privacy torts have been construed very narrowly by the courts. Some of them are referred to today as dying torts, although some of them still seem to be going strong.

Now, the concept of privacy based on the mere fact that information was spread asserted a new kind of property right in information, and Gene has already talked a little bit about this. This assertion is too broad, though, to make sense. Unlike copyright, the new right to own information about yourself or to control it amounts to a claim of ownership of facts and opinions and ideas about one's own actions, and unlike defamation, which lets you sue when someone disseminates false information, a right to own or control information about yourself gives you a veto power over truthful information.

Now, to jump ahead to today's debate, what has not been widely recognized and which makes this history of privacy and journalism relevant to the debate today is it hasn't been widely recognized the extent to which businesses, like journalists, rely on the freedom of information to produce goods and services. Also, consumers rely on information produced by businesses to learn about products. Economic studies have shown that advertising and marketing alert consumers to flaws in existing products; to the existence of new

competitors and choices in the marketplace and help bring down prices.

But many proposed privacy laws would be even much more extreme than the privacy rule attack that was initially made upon journalism. The journalists were attacked only for disseminating information to a broad public, whereas, in the case of the laws proposed today for commercial business, rather, the target is just the mere having the information or just the act of possessing it, although it may be disseminated only to legitimate businesses for their special purposes.

So in the historical context, then——

Mr. STEARNS. Ms. Singleton, can we have you wrap up?

Ms. SINGLETON. Yes, I will.

Mr. STEARNS. And then, we are going to take a break and just go vote.

Ms. SINGLETON. I will just summarize my main points. The Fourth Amendment should not be a basis for asserting privacy rights against commercial businesses, because no State action in the private sector enjoys Constitutional rights of free speech. And the second is the idea that people own or have a right to control the information about themselves is a radical departure from the free flow of information that has made the U.S. the world's leading economy. Thank you.

[The prepared statement of Solveig Singleton follows:]

PREPARED STATEMENT OF SOLVEIG SINGLETON, SENIOR POLICY ANALYST, COMPETITIVE ENTERPRISE INSTITUTE

Mr. Chairman, my name is Solveig Singleton and I am a lawyer and senior analyst at the Competitive Enterprise Institute. Thank you for this chance to comment on the history of privacy law and commercial enterprises. Based on my research,[1] I offer the following observations:

- The Fourth Amendment should not be a basis for asserting privacy rights against journalists or commercial businesses, for there is no "state action" and the private sector enjoys constitutional rights of free speech.
- The idea that people own or have a right to control information about themselves has no historical justification; it is a radical and extreme departure from the free flow of information that has made the U.S. the world's leading economy.
- Today, we take shocking uses of "private" information by journalists in stride; less sensibly, we fret about electronic databases and learning tools—although these represent a natural and beneficial evolution away from reliance on gossip and guesses about people's preferences.

U.S. Privacy Law in the Nineteenth Century. In the nineteenth century, as today, the law of privacy consists of two different sets of rules. First, there is the Fourth Amendment of the U.S. Constitution, which protects our rights against brutal searches from the government. Obviously, in the nineteenth century and today, it was not applied to the private sector.[2] The private sector has no power to seize and search one's property without consent under color of law. This remains true today. Note that there was and is no conflict between the Fourth Amendment and the First Amendment's rights of free speech. One might say that the Fourth Amendment is an example of a modified free speech right;[3] just as the Supreme Court recognized that Jehovah's Witnesses cannot be compelled to pledge allegiance to the flag, we cannot compel people to show the content of their papers and homes without a showing of probable cause. This makes the Fourth Amendment a very inappropriate basis for asserting expansive privacy rights against journalists or businesses today, who are not the government and who do enjoy free speech rights.

[1] Most of this research is documented in Solveig Singleton, "Privacy Versus the First Amendment: A Skeptical Approach," XI *Fordham Intellectual Property, Media & Entertainment L. J.* 97 (Autumn 2000).

[2] Ibid at 99.

[3] Ibid. at 104.

Second, there was a common law of privacy in the private sector. For example, privacy was recognized as an element in disputes over physical property boundaries and easements or nuisances, for example, when two buildings were built close together.[4] Because these private sector cases identify privacy with physical property rights, there is no conflict between the First Amendment and privacy; property rights mark the boundaries of free speech rights, too.[5] One's right to read books does not give one a right to steal books—or letters—from a neighbor's house or out of his pocket.

Privacy in the Early Twentieth Century. The concept of a right to privacy detached from physical property rights was not unknown during the early part of nineteenth century,[6] but it was not recognized in the courts until the early part of the twentieth century. A famous law review article by Brandeis & Warren calling for creation of a privacy tort for use against the press was cited in some of these cases.[7] Over the years, many of the four privacy torts that sprang up were often directed against journalists. It became obvious in these cases when no violation of physical property or a contract has occurred, privacy is in conflict with free speech rights. Over the years, privacy torts have been constrained narrowly by the courts; some are referred to as "dying torts."[8]

The concept of privacy suit based on the mere fact that information was spread asserted a sort of new property right in information. This expanded right has not prospered in the legal system, for it is a troubling one. Taken literally, it would obliterate the practice of journalism and much ordinary conversation. Unlike intellectual property, the new right amounts to a claim of ownership of facts and ideas. Unlike defamation, which lets you sue when someone disseminates *false* information, a right to own or control information about oneself gives you a veto power over *truthful* information.[9] And, unlike intellectual property law, an expanded view of privacy is not sanctioned by the Constitution.

Within U.S. legal history, there is little support for the concept that people own information about themselves and much support for the idea that facts and ideas and opinions are and should remain free to be communicated. This observation holds even as the focus of privacy has shifted from journalism to business. Journalist too is a commercial enterprise. And what has not been well-recognized by policymakers is the extent to which businesses, like journalists, rely on the freedom of information to produce goods and services, and the extent to which consumers rely on information produced by commercial enterprises to learn about those products. Economic studies have produced substantial evidence that advertising and marketing alerts consumers to flaws in existing products, to the existence of new competitors and choices in the market, and helps bring down prices.[10]

Broad privacy principles are represented as a moderate step towards giving consumer's "choice." In fact, these broad principles are a radical and extreme departure from the American tradition of the free flow of information. Writing broad privacy principles into a law for the commercial sector would amount to a sudden massive expansion of copyright or defamation law, a step that Congress would not dream of.

Even supposedly moderate "opt-out" measures are far more radical than they seem. The evolution of formal information networks such as consumer credit reporting has important benefits for the public as a whole. Even the poor or those who are not well known in a given community may buy on credit, a relatively recent and beneficial development. The existence of credit reports gives consumers an incentive to make payments on time, which means that businesses can lower the losses they suffer from default. Note, however, that had a statute imposing an opt-out rule been in place in the late nineteenth century when all this began, credit reporting could never have evolved! All of the bad debtors would have opted out! Similarly, on the Internet today, Amazon.com and other e-commerce distributors rely on commercial services to confirm that the addresses and names of their customers are valid, to weed out fraud. But this would be impossible if the database were full of holes and gaps left by opt-outs, well-meaning or sinister.

---

[4] Ibid at 107-114.

[5] John O. McGinnis, "The Once and Future Property-Based Vision of the First Amendment, 63 The U. of Chicago L. Rev. 49 (1996).

[6] For example, a sort of privacy right closely akin to intellectual property was protected by cases involving the reprinting of letters. Blackstone speaks of defamation by pictures, a tort closely akin to the modern privacy of placing someone in a "false light." Singleton at 110.

[7] Ibid. at 105-106.

[8] Ibid. at 111, 114.

[9] Ibid. at 114.

[10] See generally John E. Calfee, *Fear of Persuasion: Advertising and Regulation* (Agora Association, 1997).

The Evolution of Databases from The Late Nineteenth Century to Today.

Within the U.S. legal tradition that commercial enterprises are generally free to learn about and communicate with their customers, the way in which they have done so has evolved over time. Economists have documented how formal networks for checking credit and assessing the reliability of goods have grown out of informal networks. *Dun & Bradstreet,* which reports on the creditworthiness of businesses, originated with Lewis Tappan, who managed credit accounts in his brother's silk business and who exchanged letters with 180 correspondents throughout the country about the creditworthiness of businesses in their communities.[11] Forty years ago community-based nonprofit organizations handled consumer credit reporting, now handled by three nationwide for-profit firms.[12]

The formalization of the collection of information about consumers portends nothing sinister. Databases are a natural entrepreneurial adaptation to a more urban world, freed of small-town gossip.

This holds true of Internet web sites, who are at a tremendous disadvantage compared to real-space businesses. For decades, the ordinary shopkeeper with a little store on the streeet can stand at the counter and watch people come it. He can see if they are regulars or strangers, if they are locals or tourists, German or Spanish, young or old, male or female. Do they look longingly at the stuffed monkeys, but comment that the price is just a little too high? Are they missing the display in the back? The operator of a web site has none of this information. It is as if he is deaf, dumb, and blind. And thus he has little chance of improving his service to customers, unless he hits upon their needs by sheer dumb luck. Thus, cookies were born. They are more properly viewed as the eyes and ears of the Internet than as some kind of sinister surveillance device.

Many of the same arguments that were deployed against the journalist are today deployed against business uses of information. But they have no more merit than in their original context. For example, it is alleged that the transmission of information in itself and represents a threat to human autonomy and dignity. But writing a story about Madonna is not the same thing as seizing and torturing her. Receiving an unwanted advertisement in the mail is not akin to stealing someone's identity. The fact that we tolerate the rights of journalists to promulgate stories that once would have been considered shocking and indecent is a good sign that human beings are as always tough, adaptable creatures. We are not going to wither away because Safeway knows we bought lettuce. Some may be a little wary of the Internet—but if that has any basis in reality it is the fear of real crimes like identify theft, which are already illegal and for which have little to do with legitimate businesses use of information.

The fact of the matter is, human beings, whether they are consumers, voters, or businesses, rarely make better decisions with less information. Laws that view the spread of information itself as the enemy will not target any real problems, and will do considerable harm.

Mr. STEARNS. Thank you, and the committee will take a 15-minute break and resume.

[Brief recess.]

Mr. STEARNS. If I can have the attendees sit down, the committee will come to order.

We will continue with our panel, and we will start with Mr. Rotenberg, if you would be so kind as to give us your opening statement.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you very much, Mr. Chairman. I appreciate the opportunity to be here today. I am director of the Electronic Privacy Information Center. I have also been on the faculty at Georgetown Law Center, where I have taught privacy law for more than 10 years, and I have edited two books on privacy that are in use in U.S. law schools today which I would be happy to

[11] Daniel B. Klein, "Knowledge, Reputation, and Trust by Voluntary Means," in *Reputation: Studies in the Voluntary Elicitation of Good Conduct,* ed. Daniel B. Klein (Ann Arbor: University of Michigan Press, 1997): 7.

[12] Ibid.

make available to the committee and the staff if that would be useful.

What I do in my testimony is to outline what I think are the broad themes of the development of privacy law in the United States. And this really is based on my work and research and my teaching over the years to try to give you a framework to understand what it is when we talk about privacy law. The first point that I make in my testimony is that the concept of the protection of privacy in law is very much an American tradition. It is not only in our Fourth Amendment that establishes the warrant process before the government may conduct a search but even in the Brandeis-Warren tort, which was described a moment ago.

When that was first announced and reviewed by legal scholars in the early part of this century, people described it as the American tort, something unique to the U.S. legal system, to provide people a right of action against other for private acts, and the fair information practices which have also been discussed and provide the framework for many of the modern-day privacy laws both in the United States and around the world.

Those principles were first articulated in the United States in the early 1970's, and they provided the underpinnings for our Privacy Act, which safeguards the information that is held by Federal agencies and is, in many ways, the most robust privacy law in the United States. So it is critical to understand in this discussion that our starting point I don't think is really do we regulate? Don't we regulate? You know, what is the appropriate role of government? It is with the understanding that privacy, as a right in law, is very much a part of the American tradition.

The second point I would like to make is that what privacy laws typically do is to allocate rights and responsibilities. They are not simply, as Gene Volokh has suggested, a restriction on the right to talk about others. There are, in privacy laws, elements sometimes that place limitations on disclosure, and they may, in certain circumstances, I agree, raise First Amendment issues.

But if you look at the whole structure of a privacy law, whether it is the Fair Credit Reporting Act of 1970 or the cable subscriber privacy provisions in the Cable Act of 1984, you will see a number of different elements. One of the most interesting elements in a privacy law, somewhat paradoxically, is the requirement of transparency, of openness, to give individuals the right, for example, to obtain a copy of their credit report to see if the information that is being kept about them is accurate and complete, so that when they go to obtain a home mortgage or a car loan, that decision is being made based on accurate information.

And so, for example, when Fred Cate is describing the importance of access to accurate information in commercial markets, part of that accuracy comes about because individuals, by virtue of privacy laws, have the right to get access to information about them that is being used for decisions that affect their economic and employment opportunities.

The third point I would like to make, and this may surprise you a little bit, but it is very much my view that in the modern era of privacy law in the United States, as new technology has evolved, it is not the case that Congress has generally stood back and al-

lowed the technology to go forward and then wrestled with the privacy issue. It is rather the case that Congress has typically established privacy safeguards at the beginning, before new commercial services were widely adopted. This was true, for example, in 1984, when you did the Cable Act and included the subscriber privacy provisions. It was true in 1986 with electronic mail. The video rental industry, which began the late 1980's; you remember the Judge Bork bill to protect the privacy of video rental records? You did the Telecommunications Act in 1996; included new provisions to protect the privacy of customer billing information.

What is remarkable about the discussion concerning privacy on the Internet is that this is really the first instance with a new technology that Congress has decided not to legislate at the front end to protect consumer privacy and to rely instead on a mixture of self-regulatory and industry-directed initiatives. Now, I think it is an important question to explore how successful those initiatives have been, but I would like to suggest to you that one of the reasons that you may be seeing such high levels of public concern today that you see, you know, the consumer protests, literally, public protests of new consumer products is resulting in part because we have not yet established in law clear privacy standards to protect these new types of commercial transactions, and I think that is a real risk.

I make several other points in my statement, but one key point which I would like to draw your attention to concerns the use of technology. And it is my view that technology plays a very important role in protecting privacy. In fact, the first book we did was titled Technology and Privacy: the New Landscape. And there is a chapter in there that talks about the role of privacy-enhancing techniques.

My own organization has been a big advocate of strong encryption; techniques to protect your identity. But I have come to believe that it is vitally important that if you are going to talk about technical solutions to the privacy issue that you understand very clearly what the technology does and, in particular, what the impact is on the collection and use of personal information. P3P, which is an industry-backed effort, in my view, is not a privacy technology. It does not limit the collection of personal information. It facilitates the collection of personal information.

And this is an important issue for you to consider as you look at new proposals and new legislation. I think there are other technical methods that could do a better job of protecting online privacy.

As I said, Mr. Chairman, there are a few other points in my statement. I suggest also that you should look closely at the issue of whether Federal preemption is appropriate. In fact, it has not generally been done by tradition in the privacy field. It was not done recently with the financial regs or with the medical regs. I understand the interstate commerce concern, but I think you should look at some of the history here.

And finally, on the First Amendment issue, I agree with Professor Volokh. There is a real question there. But even Professor Volokh, in his article for the Stanford Law Review, I think acknowledges that some of these privacy terms, viewed as part of an

implied contract, an understanding that information provided for a purpose won't be disclosed for another purpose, are probably acceptable. And that is really all we are arguing on this point: in the context of a particular business relationship, if you provide information for a particular purpose, you would reasonably expect it would not be used for other purposes.

So thank you very much, and I will be pleased to answer your questions.

[The prepared statement of Marc Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

I appreciate the opportunity to appear before the Committee today to discuss privacy issues. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center in Washington, and I have taught the Law of Information Privacy at Georgetown since 1990. As both an advocate and academic, I have participated in many of the leading privacy debates in this country. In the spirit of this hearing, I will focus my comments on several general observations about privacy law. I'd like to emphasize at the start that this is an enormously interesting and important topic and I appreciate the decision of the Committee to begin with a discussion at a high level.

1. The Protection of Privacy in Law is Central to the American Legal Tradition

The protection of privacy in law is one of the great contributions of the American legal system. When the framers of the Bill of Rights set out in the Fourth Amendment a legal procedure that placed a judge between the authority of the state and the rights of the citizen, they established a structure that today distinguishes democratic governments from dictatorships. It is without question a burden to the police that they may not freely seize evidence, intercept phone calls, or detain individuals without probable cause, but this is a burden that every Constitutional democracy accepts as a fundamental requirement to safeguard the rights of it citizens.

But it is not just with respect to government that our country has established rights of privacy in law; we have done so also with respect to actions among private individuals, the practices of business, the use of new technology, and the collection and use of personal information for commercial purposes. When Brandeis and Warren first set out the right of privacy in the famous 1890 law review article it came to be known as the "American tort." The privacy tort became the basis for privacy claims that were recognized in state courts, state legislatures, and eventually Congress.

Our tradition of protecting privacy rights in law has carried forward with each new technology. From the telephone, to computers, cable television, electronic mail, video tape rentals. Our privacy laws, like all laws, are imperfect. But they reflect at their core a belief that we have the ability, through our government and our legal institutions, to control the technologies that we create, to ensure the we can obtain the benefits of new technology and preserve important political values.

So, when privacy and consumer advocates testify in support of restrictions on government surveillance, safeguards for financial records, and protections for consumers in electronic commerce, it is with full regard and understanding of the American legal tradition. The burden of justifying the self-regulatory approach falls squarely on its supporters. The first lesson of US law is that the presumption favors legal safeguards.

I make this point at the outset because there is a tendency in the policy debates about privacy to ask the question whether to "regulate" or what is the "appropriate role" of government. The better starting point is with the recognition that in the United States we have long understood that privacy is a right protected in law.

2. Privacy Law Allocates Rights and Responsibilities and Ensure Fairness and Transparency in the Collection and Use of Personal Information

Next we should consider what we mean when we discuss privacy laws. Some believe that privacy laws are simply a restriction on the right to speak freely. There is an aspect of privacy protection that may, in some circumstances, limit the disclosure of certain types of personal information obtained in the context of certain relations. But to view privacy law as only a restriction on publication is to misunderstand the structure, history and purpose of privacy laws in the United States.

Typically, privacy laws set out a range of rights and responsibilities for the collection and use of personal information. The Fair Credit Reporting Act, for example, does not simply limit the disclosure of information contained in a credit report, it also places on the credit reporting agency an obligation to ensure that the information is correct and timely, and it provides the subject of the credit report the opportunity to inspect the record and correct it if necessary. These responsibilities help ensure that information collected is used for its intended purposes and that determinations, such as whether a person qualifies for a car loan or can obtain a home mortgage, are based on accurate information.

The rights and responsibilities that provide the basis of privacy laws have come to be known as "Fair Information Practices." Although the specific elements that make up Fair Information Practices may vary somewhat, what is significant is the high degree of commonality of these principles, across subject matter, technologies, and jurisdictions. In many respects this is not surprising. The goal is simply to fairly allocate the responsibilities to safeguard personal information.

Not only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection. The most well known of these international guidelines are the Organization for Economic Co-operation and Development's Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"). Fair Information Practices also provided the basis for the recently concluded Safe Harbor arrangement between the United States and Europe.

3. Privacy Laws Respond to New Technologies

It is critical to understand that the recent history of privacy law in the United States is largely a story of efforts by Congress to pass laws to safeguard privacy as new technologies emerge. There is for example, the Federal Wiretap Act of 1968, the Act that limits the monitoring of private communications. There is also the Privacy Act of 1974 that established a legal framework for the records collected by the federal government and addressed the specific concern of Big Brother monitoring by means of automated databases. There are the privacy subscriber provisions of the Cable Act of 1984 (cable television), the Video Privacy Protection Act (video rental records), the Electronic Communications Privacy Act of 1998 (electronic mail), the Polygraph Protection Act of 1988 (lie detectors), and the Telephone Consumer Protection Act of 1991 (auto-dialers and junk faxes), the Children's' Online Privacy Protection of 1999 (Children's' data obtained by companies operating on the Internet). In addition, many laws at the state level are designed to further limit the monitoring of private activities in the United States.

Privacy laws have come about in response to challenges posed by new technologies. But the aim is rarely to limit the technology or to stifle a new business; it is instead to ensure that the data collection is fair, transparent, and subject to law. This approach builds consumer confidence, establishes a stable business environment, and allows for the benefits of new technology while safeguarding key interests.

4. Privacy Protection by Self-regulation is a Recent Development

Until about 1996, if one were asked to describe the US approach to privacy protection for personal information, you would likely have said there is "omnibus" protection with respect to records held by the federal government and "sectoral" protection concerning the private sector. The point is that the Privacy Act of 1974 covered all federal agencies, while regulation in the private sector had been done on a more piecemeal basis. The contrast with the European approach was also understood: Europe had adopted an "omnibus" approach for private sector records, based in part on the need to harmonize national law as part of the establishment of the European Union. In the United States there was little discussion of privacy protection through "self-regulation." There were a few efforts by trade groups to establish privacy practices, most notably the Mail Preference Service of the Direct Marking Associations, but these efforts typically came about as means to hold off legislation.

Beginning in 1996 an effort began to develop a more comprehensive self-regulatory approach to privacy protection. Companies posted policies, privacy seals were announced, new organizations were established to review privacy practices, and the FTC said it would take action against firms that failed to follow their privacy policies. This was done for several reasons, including growing public concern about the loss of privacy, fear that legislation restricting certain business practices might be adopted, and recognition that the European Union might limit the transfer of per-

sonal information about European consumer to American firms unless steps were take to establish stronger privacy safeguards.

It may be too soon to say whether this new "self-regulatory" approach will over time effectively protect the privacy of American consumers. The FTC last year concluded that while progress had been made, legislation was nonetheless required. But there are several recent developments that deserve further consideration by the Committee if there is going to be a meaningful evaluation of self-regulation. Here are five issues that I believe call into question the effectives of self-regulation:

- *The redefinition of privacy.* There has been a sharp departure from the bundle of rights associated with Fair Information Practices to a narrow characterization of privacy as simply "notice and choice" that is at odds with the tradition of privacy law in the US. Privacy notices appear to operate more like disclaimers or warning labels than any actual assurance of protection.
- *The development of intrusive new marking practices.* Profiling, tracking, and monitoring of American consumers have become far more widespread as a result of the self-regulatory approach to privacy. It is not clear yet what the impact will be on educational or employment opportunities, but there is always that risk, in the absence of legislation, that once permanent dossiers on Americans are created they will be used for purposed completed unrelated to the original collection.
- *The ability of the FTC to operate as an effective privacy agency.* The FTC appears to lack the statutory authority, the resources, and the reporting requirements that are required to operate effectively on privacy issues. There are too many complaints, too little adjudication, and too little oversight.
- *The ability to respond to new technologies.* In the next few years we are going to see the development of new technologies that both hold great promise for innovation and technical achievement as well as significant risk to personal privacy. The use of genetic information, for example, poses new challenge that may be addressed more effectively through privacy legislation than the "notice and choice" approach.
- *Growing public concern about the loss of privacy.* At least one measure of success for a policy approach must be public support. There is little evidence to indicate that the public favors the self-regulatory approach to privacy protection.

While I remain very skeptical about self-regulation to protect privacy, I want to emphasize that establishing a right of privacy in law does not necessarily extensive regulation. There are many privacy of only a few pages that extraordinarily effective. The Subscriber privacy provision in the Cable Act of 1984, for example, is one of the most effective privacy laws in the US. It provides a very good model going forward for emerging privacy issues in the commercial world.

5. Genuine Privacy Enhancing Technologies (PETs) Limit or Eliminate the Collection of Personally Identifiable Information

My fifth point is that technology does have a role to play in privacy protection, but it is critical to think carefully about the collection and use of personal information in evaluating various technical methods. To say simply "there must be technological solutions to technological problems" really does not tell us anything. Some technologies clearly exacerbate the loss of privacy, others may help restore privacy.

Over the last several years I have become particularly interested in the development of Privacy Enhancing Technologies (PETs). I have presented papers at international conferences and worked closely with several of the leading technical innovators in the world. I believe that there are methods that enable commerce and communication and that respect privacy. In my view, the goal is to promote genuine Privacy Enhancing Technologies that limit or eliminate the collection of personally identifiable information. Anonymity, for example, is critical to the future of privacy.

Of all the various approaches to online privacy, P3P may be the most problematic. It is the one privacy standard that provides no inherent privacy protection. It can as easily be used to extract data from consumers as it could be used to limit the collection of data. And I think this is fairly well understood by the industry groups that favor P3P. They do not believe that this standard will pose any significant obstacles to their plans for collecting and using persona information.

A better approach would seek to both enable commerce and to limit the collection of personal information. We have many examples of this in the physical world, from the metro card to movie tickets to the cash in our wallets. Privacy technologies should not hinder commerce but they should also not force consumers to trade privacy to participate in commerce.

6. Free Expression and Privacy Protection are Complimentary Values

On the question of the privacy and freedom of expression, this is clearly not a zero-sum relationship. This can be shown by the fact that there are many countries today with little regard for personal privacy or freedom of expression. The success of the US legal system is to preserve both interests, to safeguard free expression and to protect individual privacy.

There are also a series of cases that make clear that privacy and the First Amendment are complimentary interests. In MacIntyre v. Ohio, for example, the Supreme Court struck down an ordinance that required the publisher of a handbill to place her actual name on the pamphlet. In so doing, the Court recognized that the freedom to express ones views includes also the right to withheld ones identity. There are many other examples in American law where we safeguard privacy to promote free expression and freedom of association. It's worth noting, for example, that the freedom to vote as one wishes in a democratic society is safeguarded by the privacy of the voting booth.

There are tough cases where the First Amendment and privacy interests collide. The Supreme Court, for example, must determine this term whether the press may publish the contents of a private telephone call obtained by means of an unlawful wiretap. EPIC, my own organization, dedicated to both the protection of privacy and the promotion of free speech, struggled with the question on which side we would file an amicus. In the end, we decided it was too difficult a case. But recognizing that there are, in some instances, difficult case does not mean as a general matter that it is not possible to protect privacy and to promote free expression.

7. Federal Privacy Legislation Typically Does Not Preempt State Law

The issue of federal preemption is arising increasingly in discussions about privacy protection. It is important to understand that as a general matter, federal privacy law operates as a baseline and does not preempt stronger state statutes. This is clear from laws such the Video Privacy Protection Act of 1988 and the subscriber privacy provision in the Cable Act of 1984. This approach was reaffirmed recently in the privacy provisions of the Financial Modernization Act of 2000 and the HIPAA regulations.

There are important reasons in our form of government to continue to allow the states to operate as "laboratories of democracy." Congress may fail to act or it may act in such a way that reduces or limits the protections that a state might otherwise choose to provide for its citizens. States may also innovate and explore different approaches to common problems. California, for example, has recently passed legislation to address emerging privacy concerns and Maryland is now looking at new legislation that would provide important new protections.

8. Public Support for Privacy Protection is a Significant Consideration in the Legislative Process

In understanding the protection of privacy in America it is critical to keep in mind the central role that the Congress and the state legislatures have played in safeguarding privacy. In some instances, it has been the courts that have established rights of privacy, but more often it has been the legislature that has set out by means of statute the rights and responsibilities associated with the use of personal information in the commercial realm.

My belief is that there is today widespread public support to establish Fair Information Practices for the collection and use of personal information in the commercial sector. There is a strong American tradition to protect privacy in law, many legislative precedents and broad based public support. The question is whether Congress will accept the challenge and act to safeguard this right, described by Justice Brandeis "as the most comprehensive of all rights and the one most cherished by a free people."

I appreciate the opportunity to appear before the Committee today and will be pleased to answer your questions.

Mr. STEARNS. Professor Feldblum?

STATEMENT OF CHAI R. FELDBLUM

Ms. FELDBLUM. Thank you, Mr. Chairman, and members of the subcommittee.

My name is Chai Feldblum. I am a law professor at Georgetown University Law Center and director of the Federal Legislation Clinic, where we have worked on the issue of medical privacy for a

number of years for various organizations. But I am testifying here today in my personal capacity as a law professor—although I am used to answering questions and being grilled by students. I don't know; I guess the new generation of students is quite different—to talk about my experiences in employment discrimination and medical privacy. And instead of talking about the minute details of those areas, of which there are many, instead of getting bogged down in that to sort of step back and talk about conceptually why it makes sense for government to regulate in these areas.

Now, my written testimony gives you a description of the privacy requirements of the ADA, and I am not going to repeat those here. Basically, employers cannot ask questions of employees about their medical conditions at certain stages of the application process. They can collect a whole range of medical information before actually hiring somebody. That medical information has to be kept confidential, and employees with medical conditions are forced to disclose those conditions to their employers if they want reasonable accommodations.

So what I want to focus on is why is government regulation of privacy in this way appropriate? I think that when government regulates conduct that it is otherwise permitted to regulate, such as employment discrimination, it can also regulate speech that would lead directly to such discrimination. So, for example, government can say you can't refuse to hire someone because she is pregnant. You also can't refuse to ask someone if she is going to become pregnant.

Similarly, you can't ask applicants about their medical conditions if that means they won't get a fair chance to be considered for a job, but you can certainly find out about their medical information if that means they are not going to be qualified. None of us want to have 911 operators unable to hear. I mean, that is not the point.

Now, in the area of medical privacy, the context that we are dealing with is that patients believe that they have a confidential relationship with their medical professional, and yet, that expectation is compromised every day by the interconnected research, medical, treatment, payment, quality system that we live in. The California Health Care Foundation has done a fascinating presentation of where our medical information actually goes, and I would absolutely recommend that presentation to everybody.

Now, of course, a certain amount of individually identifiable health care information has to flow through our medical system. As someone who has represented disability organizations, I can tell you that people with disabilities have a very pragmatic view of this issue. Bottom line: they want a health care system that is effective and efficient. But precisely because the interaction in the medical system starts with a contractual relationship between the patient and the provider, the individual must feel assured of certain ground rules that their information will, in fact, be used appropriately.

Now, let me end by saying that Congress, in 1996, did tell the Department of Health and Human Services to implement nine standards, and these were standards about transaction codes and identifiers and data security, et cetera. I think it made sense for Congress to interact in this way with the private parties because

the only way to have consistent, uniform standards in the health care system is if, in fact, government intervenes and says everyone has to abide by these standards. That is what eight of those standards were about.

But at the same time, government has to make sure that privacy protections are built in as well. That is the ninth standard.

Well, I very much appreciate that you are looking at this issue, and I look forward to answering any of your questions.

Mr. STEARNS. You roughly have 2 minutes left.

Ms. FELDBLUM. Oh, I do. My thing over here says stop.

Mr. STEARNS. I just checked.

Ms. FELDBLUM. Well, then, I am going to give you my last two paragraphs.

Mr. STEARNS. There you go.

Ms. FELDBLUM. And I know that if you had gone home without them, it just would not have been the same.

I know that there is controversy about the regulations that have been put out, but for purposes of this big picture hearing, I want to stress the need to analyze privacy within the specific context of which the perceived need to regulate arises, and if there is anything that you get from this hearing and to me anything about doing—thank you; I know you agree, a big picture hearing as opposed to a hearing on a particular bill, it is to focus on the context in which that privacy concern arises.

In the health care arena, that context is a longstanding belief between patient and doctor that medical information should be kept confidential juxtaposed with the reality of a complex health care treatment, payment, research, quality and marketing system that uses a significant amount of individually identifiable information without patients' explicit consent although with some patients' dimly sensed fear.

The role of government, I believe, is to bring clarity and confidence to this area. Thus, the goal of any system of privacy regulation should be to enhance the treatment, payment, research and quality aspects of our health care system through creating a workable privacy system that gives patients trust and ensure that health care entities can engage in the marketing necessary to their financial health consistent with consumer consent.

Now, I can assure you as someone who has worked in this area for 6 years that there is a lot of debate and a lot of detail within that sentence. What is a workable system? But I think there is a common principle that there is a role for government to ensure that there are uniform, consistent standards and confidence and trust in the system. That is what you should do in the medical privacy area, and consistent with the context of these other areas, that is what you should do in other areas as well.

Thank you.

[The prepared statement of Chai R. Feldblum follows:]

PREPARED STATEMENT OF CHAI R. FELDBLUM, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER

Mr. Chairman and Members of the House Subcommittee on Commerce, Trade, and Consumer Protection:

Thank you for inviting me to testify today regarding "Privacy in the Commercial World." My name is Chai Feldblum. I am a Professor of Law at Georgetown Univer-

sity Law Center, and Director of the Law Center's Federal Legislation Clinic. I created the Clinic in 1993 with the goal of training law students to be "legislative lawyers": that is, lawyers who are equally at ease with law and with politics. My goal is to train lawyers who are steeped in law and who like reading legal text, *and* at the same time, who are sophisticated about politics, know how to speak and write in "English" rather than in "law," and who like the particular world of political negotiation. The goal is to produce lawyers who will actually be *helpful* to you and your staff as you create legislation to address the needs of our country.[1]

I also wear the traditional hat of an academic professor. My academic legal writings have been primarily in the area of civil rights, with a focus on disability law and sexual orientation and the law.

I appear before you today as an amalgam of those roles. In my life before teaching, I was the principal lawyer representing the disability community in the drafting and negotiating of the Americans with Disabilities Act—including those provisions impacting on privacy and confidentiality. As Director of the Federal Legislation Clinic, I have represented the National Association of People with AIDS (NAPWA), in its capacity as co-chair of the Privacy Working Group of the Consortium of Citizens with Disabilities.[2] For six years, we have worked on behalf of the disability community toward passage of comprehensive federal medical privacy legislation. More recently, the Clinic has represented the Family Violence Prevention Fund, which is also concerned with enhancing medical privacy in this country.[3]

Today, however, I wish to draw on those experiences to share with you some general observations about protecting the privacy of our nation's citizens.[4] I am less familiar with the academic and advocacy debate regarding proposals to regulate consumer information databanks developed by businesses (the subject of some of the writing of my co-panelists), and more familiar with the debate regarding privacy as it relates to employment discrimination and medical information. What I hope to do, therefore, is share with you some observations on the latter forms of privacy, and perhaps extrapolate from that some observations on privacy in general.[5]

A useful place to start is a sentence from my co-panelist Eugene Volokh's May 2000 article on freedom of speech and information privacy: "'[P]rivacy' is a word with many meanings, and with such words both judges and laypeople often shift from one meaning to the other even in cases where the meanings have little in common."[6] I completely agree with that observation. While I do not necessarily agree with my co-panelist's subsequent conclusion that harmful analogies are more likely be drawn if the privacy of consumer information databases are regulated,[7] I believe

---

[1] For an explication of "legislative lawyering," see "Five Circles of an Effective Coalition" and "What is Legislative Lawyering?" *available at* http://www.law.georgetown.edu/clinics/flc.

[2] The Consortium for Citizens with Disabilities (CCD) is a Washington-based coalition of approximately 100 national disability, consumer, advocacy, provider and professional organizations that advocate on behalf of 54 million children and adults with disabilities and their families. As advocates for persons with disabilities, CCD supports strong privacy protections that give health consumers confidence that their information will be used appropriately and that permit the continued viability of medical research and delivery of quality health care.

[3] The Family Violence Prevention Fund is a leading national organization that advocates on behalf of the millions of women and children who are the victims of domestic violence each year. The Fund runs several major programs that deal specifically with health care and domestic violence. As advocates for people affected by domestic violence, the Fund supports privacy protections that will give victims confidence that their personal information will be used appropriately.

[4] Thus, I appear before you today in my personal capacity.

[5] My observations with regard to employment discrimination and medical privacy should not be taken to mean that I do not believe there are also serious policy considerations for applying privacy regulation to consumer databases of non-medical information. Indeed, while I consider the work of my colleague, Eugene Volokh, see below, to be of superb quality, I believe Congress must be cautious in chilling in its own action in anticipation of some speculative long-term constitutional concern. While I have touted the advantages of Congress drafting a narrowly circumscribed bill to address a real, documented public policy evil to be remedied, so as to avoid creating an inviting target for the Supreme Court to further narrow Congressional power, see testimony of Chai R. Feldblum before the Senate Judiciary Committee on the Religious Liberty Protection Act, September 9, 1999, I have never believed that Congress should fail to act when there is a clearly defined public policy problem and the recommended legislative response is not clearly unconstitutional. Of course, as Congress acts, it is useful to have the background analysis of scholars such as my co-panelists who may entertain some doubts about such actions.

[6] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You,* 52 Stan. L. Rev. 1049, 1102 (2000) (hereinafter *Freedom of Speech*).

[7] Volokh argues that "once restrictions on people's speech are accepted in the name of 'privacy,' people will likely use them to argue for other restrictions on 'privacy' grounds, even when the matter involves a very different sort of 'privacy.'" *Id.* at 1102. By contrast, my colleague at Georgetown University Law Center, Julie Cohen, has written some interesting pieces presenting a different point of view. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the*

he has helped enhance the practical debate about privacy by illuminating its various meanings and components.[8] What I would like to do is focus on two areas where the concerns are somewhat different, I believe, than those that arise in the context of consumer information databases. The best way for Members of Congress to carry out the hard work of figuring out what legislation to pass (and how to craft such legislation) depends, I believe, on developing a sensitive understanding of the context in which various privacy concerns arise.

The two areas on which I would like to focus are employment discrimination and medical privacy. Again, I do not plan to focus on the minute details of these areas (and there are a number of very minute details in each of these areas, I assure you), but rather, on the broad conceptual reasons for the enactment of legislation in these areas. Indeed, in both employment discrimination and medical privacy, Congress has already acted to some extent—and there are lessons to be drawn from those enactments.

During passage of the Americans with Disabilities Act (ADA), Congress chose to draw on Section 504 of the Rehabilitation Act of 1973, a law that prohibits programs that receive federal funds from discriminating on the basis of disability. That law, and the regulations issued pursuant to the law, provided Congress with a 17-year track record of substantive non-discrimination principles on the basis of disability. Section 504 was not focused on privacy, and yet the law included some important privacy components that were carried over to the ADA.

Congress recognized that people with hidden disabilities (such as breast cancer or HIV infection or diabetes) often do not get the chance to be fairly considered for a job because the employer finds out—through questioning at an interview or through a medical examination or questionnaire—that the applicant has a particular medical condition. In such cases, the employer may choose not to hire the person because of unsubstantiated fears regarding the person's possible absentee rate or the response of co-workers, or because of possibly substantiated fears of higher health care costs that might be associated with that individual. In either case, in such circumstances the individual is judged not on the *merits* of his or her ability to *do* the job, but rather on ramifications that (justly or unjustly) flow from the individual's medical condition.

In some cases, of course, an individual's medical condition will impact directly on the person's ability to perform the job. For example, we all want our airline pilots to be able to see, our truck drivers to be able to drive, and out "911 operators" to be able to hear.

The ADA thus creates privacy rules that ensure applicants are provided a *fair* chance to be *considered* for a job, but also ensures that employers are permitted to hire only *qualified* employees. Under this framework, employers may not ask job applicants to disclose their medical conditions during the initial stages of an application process. Rather, after a conditional job offer is extended, employers may ask applicants to respond to questions about their medical conditions (or to take a physical examination)—and based on that information, employers may refuse to hire employees who are not qualified for the relevant jobs.[9]

Subject as Object, 52 Stan. L. Rev. 1373 (2000); Julie E. Cohen, Privacy, Ideology, and Technology: A Response to Jeffrey Rosen, 89 GEO. L. J. xx (2001)(forthcoming). *See also* Janlori Goldman, *Privacy & Individual Empowerment in the Interactive Age,* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE (C. Bennett & R. Grant eds. 1999).

[8] The work of my other co-panelists has also been of significant use in this regard. *See, e.g.,* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach,* 11 Fordham Intell. Prop. Media & Ent. L. J. 97 (2000) (hereinafter *Privacy*); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States,* 33 Ind. L. Rev. 173 (1999); Wayne Madsen, David L. Sobel, Marc Rotenberg, David Banisar of The Electronic Privacy Information Center, *Cryptography and Liberty: An International Survey Of Encryption Policy,* 16 J. Marshall J. Computer & Info. L. 475 (1998).

[9] 42 U.S.C. § 12112(a)-(c). The ADA had originally incorporated a stricter rule which permitted employers to request from applicants only that medical information which was directly related to the job. After negotiations with the business community and the Bush Administration, however, that provision was modified to allow employers to request any medical information. Chai Feldblum, *Medical Examinations and Inquiries Under the Americans with Disabilities Act: A View from the Inside,* 64 TEMPLE LAW REVIEW 521, 535-537 (1991) (hereinafter *Medical Examinations*). The key protection for people with disabilities, however, is that the medical information must demonstrate they are not qualified for the job. Whether a person is qualified for a job will depend on whether there are reasonable accommodations that will enable the person to perform the job functions. 42 U.S.C. § 12112(b)(5)(a); *see generally,* Chai Feldblum, *Anti-discrimination Requirements of the ADA,* IMPLEMENTING THE AMERICANS WITH DISABILITIES ACT: RIGHTS AND RESPONSIBILITIES OF ALL AMERICANS (L. Gostin & H. Beyer eds. 1992).

Once employers have collected medical information about applicants through such questioning or examinations, that information must be kept confidential.[10] In addition, if an employer seeks medical information from an employee on the job,[11] that information similarly must be kept confidential. What that means is the following. If medical information indicates that an applicant is not qualified to perform a job, or that an employee is no longer qualified to perform the job, the medical information may be used to refuse to hire or to fire that applicant or employee. This includes, obviously, disclosing the medical information to the relevant person with employment authority. However, if the medical information does not indicate that an applicant or employee is unqualified for a job, then that information cannot be circulated within the employment setting.[12]

There is a flip side to the confidentiality requirements of the ADA. Many people with medical conditions wish to keep their conditions private, and do not wish either their employer or their co-workers to know of their conditions. Often, this does not pose a problem. However, in certain circumstances, an employee is *required* by law to *divulge* his or her condition, even if such disclosure is personally difficult for the individual. These circumstances arise when an employee seeks a modification of an employment practice or procedure (a "reasonable accommodation") because of his or her medical condition. Thus, for example, if an employee has a health condition that requires her to receive a two-hour treatment once a week, and she seeks time off to receive that treatment—she *must* disclose the existence and nature of her health condition in order to receive the benefit of the reasonable accommodation requirement under the ADA.[13]

What can we extrapolate from these employment requirements? As I noted, it is important to view privacy issues in the *context* in which they arise. When government regulates conduct that it is otherwise permitted to regulate (for example, prohibiting discrimination in employment contracts based on race, sex, or disability), I believe it is also permitted to regulate speech that would directly *contribute* to such discrimination. Thus, the government may not only prohibit an employer from discriminating on the basis of pregnancy, but may also prohibit an employer from asking a prospective job applicant if she is planning to become pregnant.[14] Similarly, employers may be restricted in the questions they ask of applicants regarding their medical conditions during the application process.[15] These restrictions should be narrowly tailored, however, to the harm sought to be prevented by the government. For example, such tailoring is evident in the structure of the ADA, which permits employers to seek medical information prior to actually hiring an individual.

The context of the employment relationship also justifies the fact that government *compels* certain speech on the part of some employees with disabilities. As a general matter, of course, government may not compel speech on the part of its citizens.[16] But if an individual enters a contractual relationship with an employer, in which certain facets of that relationship are regulated by the government, then that individual can be expected to conform to expectations in the relationship that have been established through the government regulation. Thus, for example, although an individual must forgo some privacy rights if she wishes to take advantage of the rea-

---

[10] 42 U.S.C. § 12112(c)(3)(B).

[11] After an employee is on-the-job, medical inquiries may only be made if they are job-related. 42 U.S.C. § 12112(c)(4)(A); Feldblum, *Medical Examinations,* at 538-540.

[12] The only individuals who may gain access to these records are: supervisors who may be informed regarding necessary restrictions or reasonable accommodations; first aid and safety personnel, when appropriate, and government officials investigating compliance. 42 U.S.C. § 12112(c)(3)(B). According to regulations issued by the Equal Employment Opportunity Commission, employers may also provide such information to worker's compensation offices upon the filing of a claim by an employee. See EEOC Interpretive Guidance to 29 C.F.R. § 1630.14(b).

[13] EEOC Interpretive Guidance to 29 C.F.R. § 1630.9.

[14] See EEOC Sex Discrimination Guidelines, 29 C.F.R. § 1604.7 (1983); *King v. TWA,* 738 F.2d 255 (8th Cir. 1984).

[15] I do not believe there is much disagreement that speech which effectively constitutes an *act* of discrimination is within government's legitimate power. For example, government may not only prohibit employment discrimination based on race, but may also prohibit an employer from running an ad that seeks "whites only" for a job. The more complicated question is whether, consistent with the First Amendment, government may also prohibit employers from engaging in speech that might lead directly to such discrimination. As noted, I believe government may legitimately do so. In some cases, however, the context in which this speech arises may well be determinative. For example, in *U.D. Registry, Inc. v. California,* 40 Cal.Rptr. 2d 228 (Ct. App. 1995), a state court held that the government could not prohibit only credit reporting agencies from disclosing information regarding certain housing actions, which were otherwise a matter of public record. While I have some questions regarding the outcome of this case, the fact that the relevant information already existed in the public domain was critical to the court's decision.

[16] *See Wooley v. Maynard,* 430 U.S. 705 (1977); *West Virginia State Board of Education v. Barnette,* 319 U.S. 624 (1943).

sonable accommodation requirement of the ADA, that trade seems both appropriate and within the government's power.

A contractual relationship also exists in the area of medical privacy more generally. That relationship has led some commentators, who are otherwise leery of governmental regulation of privacy, to view medical privacy in a different light. Let me take two of my co-panelists as an example. Eugene Volokh has observed that "one sort of limited information privacy law—contract law applied to promises not to reveal information—is eminently defensible under free speech doctrine." [17] Volokh notes that this protection should also cover implied contracts and explains the relevance of this for the medical context:

> This explains much of why it's proper for the government to impose confidentiality requirements on lawyers, doctors, psychotherapists, and others: When these professionals say "I'll be your advisor," they are implicitly promising that they'll be confidential advisors, as least so long as they do not explicitly disclaim any such implicit promise.[18]

A similar observation is made by Singleton in her critique of analyzing privacy primarily as a "right to 'control' information about oneself." [19] As Singleton observes:

> This idea is familiar in medical and legal ethics and perhaps in other special professional relationships. In these relationships the expectations makes sense. The legal and medical professions understand that clients and patients will not confide in them without the right of confidentiality. Even if this right did not exist by statute, it is implicit in the agreements under which a doctor treats his patients or the lawyer counsels his clients. This understanding is informed by decades or even centuries of custom.[20]

The reality, of course, is that the confidential relationship patients believe they have with their medical professionals is compromised every day by the reality of the interconnected medical, research, payment, and marketing system that we live in. The California HealthCare Foundation has developed a fascinating presentation that graphically displays the flow of our medical information in our existing interconnected systems.[21] Thus, for example, during and following one visit to a hospital, a patient's individually-identifiable health information may be sent to a lab, a pharmacy, a pharmacy wholesaler, a drug company, a marketer, an imaging center, a primary care group administrator, a third party administrator, an insurance company, a research institution, a public health department, a medical information bureau, a life insurer, a state insurance board, an oversight or accreditation board, and an employer.

Of course, a certain amount of individually-identifiable health information must flow freely in our health care system in order for the system to work efficiently, effectively, and at a high level of quality. As someone who has represented disability organizations over the years, I can assure you that people with disabilities have a very pragmatic view of this issue. People with medical conditions tend to interact a significant amount with the medical system. Hence, they want an effective, efficient, and high quality health care system, together with the best that increased research and disease management can offer.

But disability rights advocates do not experience their desire for medical privacy to be in conflict with their desire for an effective health care system, and thus they do not view these interests as needing to be "balanced" against each other. Rather, precisely because the interaction with the medical system is, at first onset, a contractual relationship—the interaction works best if patients feels assured of certain *ground-rules:* that their individual medical information will not be disclosed to entities that may use that information to harm them; that their information will be used, within the health care system, in an "appropriate manner;" [22] that they will

---

[17] Volokh, *Freedom of Speech,* at 1057.

[18] *Id.* at 1058.

[19] Singleton, *Privacy,* at 122.

[20] *Id.* at 122-123.

[21] I watched this presentation at a conference sponsored by the California HealthCare Foundation in December 2000. It is one I would whole-heartedly recommend to Members of Congress and their staff. A useful summary graphic of "sample data flow" was developed by the Georgetown University Health Privacy project, based on the presentation of the California HealthCare Foundation, and is attached to this testimony.

[22] I put "appropriate" in quotation marks because the debate over health care privacy regulation sometimes concerns the scope of the activities over which patients should be able to control transfer of their individually identifiable information. There are many activities that patients may not realize, at first blush, are "appropriate" uses of their medical information, and yet, such activities may be quite essential for the workings of the health care system. For this reason, the debate often focuses on what providers and plans may legitimately demand—as a pre-condi-

Continued

be provided information about what those "appropriate" uses will be, and that they will have the opportunity to review their own medical records. Thus, establishing an effective system of privacy regulation can enhance the operation of the health care system by increasing individuals= trust and confidence in the initial medical contractual relationship.[23]

As in the area of employment discrimination, Congress has already acted to some extent in the area of medical privacy—although there is work that still needs to be done. In 1996, Congress directed the Department of Health and Human Services (HHS) to develop nine administrative simplification standards for use in the health care system. These standards were to address: "transaction codes and medical data code sets; consistent identifiers for patients, providers, health plans, and employers; claims attachments that support a request for payment; data security; enforcement" and "information privacy."[24] As the General Accounting Office described this Congressional mandate: "Taken together, the nine standards are intended to streamline the flow of information integral to the operation of the health care system while protecting confidential health information from inappropriate access, disclosure, and use."[25]

Congress' action to date in this area reflects, I believe, an appropriate interaction between government and private contractual parties in the health care system. Given the interconnectedness of our health care system, and the increasing use of computer technology, all parties benefit if there are consistent and uniform standards that will be used by all parties to health care transactions. To create such uniformity and consistency—and hence, administrative simplification—government must intervene through the establishment of standards to which all parties must conform. However, as government *facilitates* the uniform entry of our medical information into this administratively simplified system, it must *simultaneously* ensure that privacy standards, policies, and protections are built into the system as well.

Congress took that initial step in 1996, and the Department of Health and Human Services fulfilled its obligation in 2000. While I, as others, are disconcerted that the process will be reviewed yet again,[26] I have no doubt that, as Secretary of HHS Tommy G. Thompson has stated, after reviewing public comments, he intends to "put strong and effective health privacy protections into effect as quickly as possible."[27] I believe the Secretary, as well as the heath care industry, clearly recognize that effective privacy protection facilitates and enhances the doctor-patient relationship.

The reality, of course, is that Congress has not yet acted to ensure that medical privacy protection will exist—as a reality—in *all* contexts in which problems of disclosure may arise. For example, the mandate Congress handed to HHS covered only a select group of entities in the health care system (health care providers, health plans, and health care clearinghouses), and did not cover a range of other entities (such as employers, educational institutions, and financial institutions) that also obtain medical information. While the regulation issued by HHS makes some effort to address subsequent disclosures by such entities, I believe most observers consider there is room for improvement in this area.

The actions that Congress has previously taken in the area of medical privacy, together with the work that remains to be accomplished, provides us with some general observations on the role of government in this arena. As I stated at the outset,

---

tion for treating a patient or paying for such treatment—as they enter the contractual relationship with the patient.

[23] A national survey released in January 1999 found that one in six Americans engages in some form of "privacy protective behavior" because he or she is afraid of confidentiality breaches regarding sensitive medical information. These activities include withholding information from health care providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and avoiding care altogether. California Healthcare Foundation, *National Survey: Confidentiality of Medical Records* (January 1999). The survey was conducted by Princeton Survey Research Associates. Results are available at http://www.chcf.org/conference/survey.crfm.

[24] Ms. Leslie G. Aronovitz, Director, Health Care-Program Administration and Integrity Issues, U.S. General Accounting Office, Testimony before the Senate Committee on Health, Education, Labor, and Pensions, February 8, 2001, at 2. The mandate on HHS to implement an information privacy standard was triggered only if Congress failed to enact comprehensive medical privacy legislation by August 21, 1999. Of the nine standards required to be issued, HHS has issued a regulation governing electronic transactions (on August 17, 2000) and a regulation governing information privacy (on December 28, 2000).

[25] *Id.*

[26] See Robert Pear, "*Health Secretary Delays Medical Records Protections*," NY Times, February 27, 2001, at A14 (reporting that HHS Secretary Tommy G. Thomson announced he would seek additional public comment on the privacy regulation issued by HHS in December 2000).

[27] *Id.*

"privacy" must be viewed within a specific context. In the health care arena, that context is a long-standing belief between patient and doctor that medical information *should* be kept "confidential," juxtaposed with the *reality* of a complex health care treatment, payment, research, quality and marketing system that uses a significant amount of individually identifiable health care information without patients' explicit knowledge (albeit presumed by some patients with some dimly sensed fear). The role of government, I believe, is to bring clarity and confidence to this area. The goal of any system of privacy regulation must be to *enhance* the treatment, payment, research, and quality aspects of our health care system through creating a workable privacy system that provides patients with trust in their health care system, and at the same time, ensures that health care entities can engage in the marketing necessary to their financial health in a manner consistent with consumer consent.

Obviously, this is not necessarily an easy project. For example, while I doubt many observers of the current health care privacy debate would quibble with the first part of my previous sentence, I expect there would still be debate regarding what is a "workable system" of privacy regulation, what requirements "enhance" research or simply make life more "convenient" for researchers, and whether one uniform federal standard, with no state variations, is an essential component of such a system. Moreover, I am sure there would be disagreement regarding the extent of marketing that should be permitted without consumer consent. Nevertheless, I believe there is a shared conceptual principle that it is legitimate for government to intervene in this area so as to enhance patient trust in the health care system. The fact that this may be a hard job for government to do has never been a reason not to tackle it.

Let me conclude with some comments on an area that represents one of those "hard jobs" that need to be tackled—and that brings together some of my observations on employment discrimination and medical privacy. We are blessed to be living in a century where amazing medical and scientific advances are made every year.[28] The success of the Human Genome Project is one example of such an astonishing scientific breakthrough. But the researchers in that project, and in comparable private sector projects, correctly warn us that "genetic testing" and "genetic markers" must be treated with caution. The existence of a "genetic marker" does not necessarily mean an individual will develop a particular disease.[29] Moreover, employers and insurance companies may begin to view genetic information as useful information to compile, and then act upon such information for purposes that the general public, and Congress, may well find objectionable.[30] The principles that I articulated above should, I believe, lead Congress to clearly prohibit unjustified discrimination based on genetic markers for health conditions (as well as for the health conditions themselves), and to ensure that any medical privacy regulation clearly encompasses protection for genetic information.

Thank you for your attention. I look forward to responding to your questions.

Mr. STEARNS. Thank you.

Let me start with my questions. Professor Volokh, this is perhaps a more legal question, but I think our committee should tackle this and get the nuances here. What legal considerations would creating a property right in personal information trigger?

Mr. VOLOKH. Sure; this is one of the arguments that is sometimes made in support of information privacy speech restrictions, that they just create a property right in personal information. The Supreme Court has said that certain kinds of speech restrictions—specifically, copyright law is the best example—are justifiable on

---

[28] Of course, the existence of such breakthroughs only makes the reality of "medical mysteries" that much more heartbreaking. *See, e.g.,* Jerome Groopman, SECOND OPINION: STORIES OF INTUITION AND CHOICE IN THE CHANGING WORLD OF MEDICINE (2000); Jeff Wheelwright, THE IRRITABLE HEART: THE MEDICAL MYSTERY OF THE GULF WAR (2001); Hillary Johnsen, OSLER'S WEB: INSIDE THE LABYRINTH OF THE CHRONIC FATIGUE SYNDROME EPIDEMIC (1996). Nevertheless, medical advances continue to help a large number of individuals.

[29] For background information on the Human Genome Project and genetic research generally, see the website of the National Human Genome Research Institute at the National Institutes of Health, available at http://www.nhgri.nih.gov.

[30] Certain evidence seems to indicate that such activities are already taking place. See, e.g., U.S. Equal Employment Opportunity Commission, "EEOC Petitions Court to Ban Genetic Testing of Railroad Workers in First EEOC Case Challenging Genetic Testing Under Americans with Disabilities Act," available at http://www.eeoc.gov/press/2-9-01-c.html.

an intellectual property rationale. But in that case, Harper and Row v. Nation Enterprises, where the Court upheld copyright law, it said many times that the reason that copyright law is Constitutional is precisely because it distinguishes facts, which nobody can own under copyright law, from expression of those facts.

So if you are a historian, and you uncover some facts about a person or about something else, you have no property right in those facts. You do have a property right in the book that you used to express those facts, so nobody can copy literally or even paraphrase the book, but they can borrow the facts from your book. That is the fundamental rule of intellectual property law, but it is also a fundamental rule, as I read Harper and Row, of First Amendment law: that to the extent the intellectual property rules do survive First Amendment scrutiny, it is precisely because they do not create a monopoly in facts.

And also, if you think about what are the implications of saying that somebody has a property right in personal information? If somebody really does have a property right in personal information, that is like a property right to stop other people—not just in the business context but also, say, in the press context—from writing about this person, from communicating that information.

Mr. STEARNS. So I am on a computer. I go to a site——

Mr. VOLOKH. Yes.

Mr. STEARNS. [continuing] they send a cookie, and they start to track me, and they provide—they have a pretty good idea all about me in terms of from a marketing standpoint. At what point do I have a right to ask that they tell me what they are doing with it and to say I want to opt out?

Mr. VOLOKH. Okay; I think that there are two distinctions here. One is between data gathering of certain kinds.

Mr. STEARNS. Okay; which is——

Mr. VOLOKH. So, for example, if they pop a virus in your computer——

Mr. STEARNS. Right.

Mr. VOLOKH. [continuing] well, that would clearly be something that can be regulated.

Mr. STEARNS. Okay.

Mr. VOLOKH. But the other distinction is between disclosure requirements——

Mr. STEARNS. Okay.

Mr. VOLOKH. [continuing] and actual restrictions on communication. I think it would be quite Constitutional for Congress to say that before somebody——

Mr. STEARNS. Starts tracking you.

Mr. VOLOKH. [continuing] gathers information, they have to explain what they are doing.

Mr. STEARNS. So Constitutionally, I would have a right for them to put up a dialog box saying that I have the right to opt out?

Mr. VOLOKH. It would be Constitutional for Congress to create this as a statutory right.

Mr. STEARNS. Okay; so, it would be Constitutional.

Mr. VOLOKH. But I should mention the opt-out thing. I mean, it seems to me the site has to have the right to say look: if you want to use our site, you have to understand that we are going to reveal

this information. So I think the opt out is the customer's right not to use that site.

Mr. STEARNS. Let me follow up. Can you take us through the Constitutional tests that a court would apply regarding a law restricting commercial speech? What would qualify as compelling in your mind?

Mr. VOLOKH. Sure; if we are talking about commercial speech, which is a legal bit of shorthand that really means commercial advertising, then, there is this four-part so-called Central Hudson test which demands only a substantial government interest to justify restriction on commercial advertising. Most of this data gathering and communication does not involve commercial advertising or commercial speech under the Court's precedents.

Just like the Wall Street Journal reports speech about commerce; reports speech about commercial entities, that is not commercial speech. The Wall Street Journal is fully protected as to its data that it contains even though not as to the advertisements.

Likewise with this information that is gathered about people. If there is an advertisement that is sent to people, that is commercial speech. That can be restricted under this more lenient test. But if all we are talking about is communication of information about people, that is not commercial speech, and that requires the highest level of Constitutional scrutiny.

Mr. STEARNS. So I am on the Website, and after 3 or 4 months, I am starting to get all of this advertising. It is coming into my Website, and, you know, I don't know where it is coming from.

Mr. VOLOKH. Yes.

Mr. STEARNS. It is not only the mundane stuff, but it is starting to get more nuanced into all kinds of things——

Mr. VOLOKH. Yes.

Mr. STEARNS. [continuing] I don't want to have on my Website, and I don't understand how it got there. So is that commercial speech Constitutionally acceptable, and can I object to that?

Mr. VOLOKH. Yes; if it is advertisement that is being sent to you, not just communication about you to other people but advertisements, commercial advertisements being sent to you, that is commercial speech. Congress has somewhat more flexibility in restricting that. So, for example, Congress could certainly require that commercial ads have some disclosure requirement, for example, explaining where it is coming from, maybe even where they got the data from you and such.

Mr. STEARNS. Because I see all of this come on, and I don't know where it is coming from. And, you know, it is okay and doesn't bother me, but after awhile, it does start to bother me.

Mr. VOLOKH. Yes; and one thing that Congress could do—and again, it is an interesting question as to whether, as a policy matter, it is a good idea for it to do, but it could give you the right to say stop sending me this stuff.

Mr. STEARNS. Right, like spamming.

Mr. VOLOKH. There is a Supreme Court case—exactly; there is a Supreme Court case 30 years ago called Rowen v. Post Office Department that had to do with paper spam.

Mr. STEARNS. Okay; one question, and then, I am done.

Professor Cate, and perhaps this is a question for each of you to answer just yes or no to, if I can, pin you down here as law professors.

As a member of the FTC's Online Access and Security Advisory Committee, you closely studied the issue of access and security as it relates to online Websites. What problems did the committee see with the access and security as it relates to consumer data? Does that make sense?

Mr. CATE. Yes, it makes perfect sense. I would like to be able to answer yes or no to that. But there were obviously numerous problems. That is one reason the committee never reached a consensus or a resolution on that issue; beginning with the problem of, first of all, how do you authenticate who you are providing access to? If somebody comes to you and says I want access to my information, how do you know who they are?

A second problem of do you have to bring together more information in order to provide them access? So, for example, if you collect information in three different ways or three different sides, you never bring it together for any purpose whatsoever, marketing or others. Would access requirements require that the business profile you in order to respond to your request for access; you know, a third being the related security issues: how do you protect the security of that transaction?

A fourth concern, particularly in the online environment, being, as this committee well knows, computers, you know, tend to collect a lot of information, much of which is never used for any purpose. For example, you know, there are backup tapes that record virtually all of the access to any Website. I am sure that is true for the Congress as well. That is not used for any purpose at all. Yet, that is certainly personally identifiable information about you. Would an access request require that the institution, the business, go back and mount all of those tapes and run them in order to find data which is not used for any purpose whatsoever?

And, you know, I guess finally the fifth issue raised in that committee's discussion is what information would you have access to? You know, only personally identifiable information? How about calculated information? If I know that you purchase beer, statistically, that means you are likelier to purchase diapers. Don't ask me why. That just happens to be true.

So, if I have calculated that you are likely to have children—does that mean I have to disclose that to you?

If it is a credit score, do I have to tell you how I arrived at that score? If it publicly available information, you know, I matched some information about you with data from the public record, do I have to give you access to that information even though I am not the custodian of it and can't correct it in any event? And what if it is information that you can't correct in any event, for example, records of past transactions? You want to say you did not make that purchase at my store. You know, you can want to say that all you want. Unfortunately, you know, if I believe you did, and I can support that, I am not going to change it. Should access be provided to that type of information?

Mr. STEARNS. Well, my time has expired.

Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman.

I would like to follow up on the Chairman's question a little bit to you, Professor Volokh. I am not so concerned about advertising that comes onto folks' Websites. What I am concerned about is the topic of the discussion today, which is privacy. And from what I heard you say in your opening statement, it sounds like your view is that there is really pretty much an unrestricted First Amendment right to privacy which you can have either an expressed or an implied contract by the providers to restrict that somewhat, but if there is no contract, then, what it sounds to me you are saying is that once someone gives over, say, their medical records or their financial records that there is an unrestricted First Amendment right. Is that not accurate?

Mr. VOLOKH. My view, being kind of an extremist by temperament, my view is that——

Ms. DEGETTE. I noticed that.

Mr. VOLOKH. Exactly; is that in fact, once information is revealed without any contractual obligation to somebody, that person is free to pass it on.

Ms. DEGETTE. So, for example, if I give my medical records to somebody, and then, they, without my knowledge, transfer them to someone else, that third party, in your view, has an unrestricted First Amendment right to disseminate those records——

Mr. VOLOKH. Yes.

Ms. DEGETTE. [continuing] anywhere they want, and Congress could pass no law to control that action?

Mr. VOLOKH. A very similar question is before the U.S. Supreme Court right now. It has to do with whether the media are entitled to publish information that was illegally gathered, in that case by intercepting cellular conversations but turned over to them. And I think the answer is, for example, if a newspaper get somebody's record, they are entitled to publish it.

Ms. DEGETTE. So your answer to my question is yes, that is your view.

Mr. VOLOKH. My view is but there is also another possibility.

Ms. DEGETTE. Yes or no.

Mr. VOLOKH. My personal view, yes.

Ms. DEGETTE. What do you think about that, Mr. Rotenberg? And then, I will ask you, Professor Feldblum.

Mr. ROTENBERG. I think it is generally correct, but there are competing legal principles, and one competing legal principle is the privacy tort, particularly with regard to the disclosure of private facts. Now, that tort creates First Amendment questions, because that is the issue that you have to consider. If I know, for example, that someone is AIDS-positive, and I publish this information, it is a true fact. Assuming it is a true fact, all First Amendment theory says why would we restrict the publication of true fact? There is no defamation.

But if you go back to the concept articulated in the Brandeis and Warren article, we might restrict the publication of true facts because of the harm that it does to the individual as a person, whether or not there is identifiable economic damage, that somehow, we value the person's integrity, their autonomy and their dignity. And so we have, in American common law, recognized this privacy tort.

We have created a very high standard. The disclosure has to be very highly offensive.

And just, you know, by way of counterexample, one of the cases I teach is a case called Legg v. Wal-Mart.

Ms. DEGETTE. Right.

Mr. ROTENBERG. It concerns a woman who went into a Wal-Mart to have her vacation film developed. It included some pictures of her in the shower, of her and a friend taking a shower without any clothing on. She got back from Wal-Mart and a notice which said I am sorry; we can't process this film. She didn't think anything of it until she later learned that pictures from that roll of film were circulating in the community, because the technician who had access to that roll of film had gone ahead, developed the pictures, and circulated them.

And she brought an action against Wal-Mart. There was nothing in the agreement with Wal-Mart that said that they were prohibited from disclosing this information. The question that was put to the Minnesota Supreme Court was does she have a right of privacy——

Ms. DEGETTE. And what was the answer?

Mr. ROTENBERG. And the answer was yes.

Ms. DEGETTE. Thank you.

Professor Feldblum?

Ms. FELDBLUM. Yes; I think you have touched on exactly what I thought was the weakness when I read my colleague's article. I believe that the government does have a right to restrict that information of the newspaper or some other third party because they have a compelling interest in protecting that information, and it is narrowly tailored to that.

The contract model gets you only so far in the medical world. It is the reason why we have to be concerned that only gets you so far in terms of binding individuals. I believe Congress can bind not only the physician or the hospital to their express or implied contracts but also other entities that get that information, even though it is a burden on their speech. But you can burden speech when it is narrowly tailored to a compelling government interest, and in my mind, this is one of those.

Ms. DEGETTE. Thank you. Ms. Feldblum, let me follow up. I spoke in my opening statement about these new HIPAA regulations and have been hearing from a lot of businesses that they will be overburdensome and costly. I would be interested, and I know you were involved in the development of those regulations, and I am wondering what your thoughts are on that and if you have been thinking of ways we could streamline them to make them more workable.

Ms. FELDBLUM. I think they will cost money. The bottom line is things cost money when you actually change norms. There is a norm right now in the medical community which is that information flows very freely, and it flows that way because people think that they are all doing a good thing.

You know, often, they are, but sometimes, it doesn't make sense to have all that information flowing in that way. What the health industry said to Congress in 1996—well, they had been saying it for some time—is we have got so much information going on out

there, and we have people putting it in all of these different formats, and that is a problem for us. So we want you, government, to intervene and create standards about what the data codes should look like and what the identifiers——

Ms. DEGETTE. Well, my time has expired.

Ms. FELDBLUM. Yes, I see.

Ms. DEGETTE. So I would like to get an answer, which would be are you involved or willing to look at ways we can modify those regulations to make them more workable for industry?

Ms. FELDBLUM. I believe that the comments actually took in those concerns already and that they have been modified. I think it is unfortunate that the Secretary is opening it up for comment again. I will be involved in this 30-day comment, and if we get something better, I am all for it.

Ms. DEGETTE. Great; thank you.

Mr. STEARNS. Thank you. I thank my colleague.

Mr. Buyer?

Mr. BUYER. Thank you.

In my mind, when it comes to issues of privacy, it is easier for me to understand this when there is a contract or physical property. I am going to move into a difficult arena for me, and I am going to turn to you, Professor Volokh, only because I remember your testimony to us before the Judiciary Committee, and I appreciated your past witnessing.

What are some examples of an implied contract with an inferred privacy where there would be an unjust enrichment?

Mr. VOLOKH. A classic example of an implied contract, I think, would be a situation where——

Mr. BUYER. Well, Wal-Mart immediately comes to my mind.

Mr. VOLOKH. Exactly, exactly. I am not sure unjust enrichment is present there, but I don't think it needs to be present in order for the government to be able to act, either through a standard contract claim. You could have a claim on an implied contract without unjust enrichment; or through special tailored legislation.

I'd be happy to talk further to the unjust enrichment question, but I just don't think it is necessary as a doctrinal matter.

Mr. BUYER. An example, then. If we are to do absent physical property or a contract, in the arena of a privacy tort, is it possible to have an inferred privacy?

Mr. VOLOKH. I think the term inferred usually arises in the context of a contract; that is, a promise on somebody's part.

Mr. BUYER. Right, and I am saying absent that.

Mr. VOLOKH. Right; I oppose——

Mr. BUYER. If the courts are going to be narrowly constrained?

Mr. VOLOKH. Yes.

Mr. BUYER. Is it possible to have an inferred privacy absent?

Mr. VOLOKH. I oppose the Warren-Brandeis privacy tort. I think that there have been quite a few cases in which it has been applied in a way that, as people would predict, involved judges telling newspapers what they may and may not publish. I think that is not a good thing for a judge to do.

Mr. BUYER. People believe—they have these expectations——

Mr. VOLOKH. Yes.

Mr. BUYER. [continuing] of privacy.

Mr. VOLOKH. Yes.

Mr. BUYER. Is it possible to have an inferred privacy, absent—I mean, in a privacy tort, can you have an inferred privacy?

Mr. ROTENBERG. If I may answer, Mr. Buyer, I think the Internet today provides a wealth of very interesting examples to answer the question that you are asking, and the reason for this is that there is a great deal of surreptitious data collection taking place by Websites, by firms that do advertising profiling, the so-called Web bugs that are related to HTML tags that make it possible to track and collect data about individuals without their knowledge. Now, this is a very interesting type of data collection, because I think you could fairly say that there is really no contractual relationship, and what was quite significant about the Double-Click example is that an advertiser really exists apart from the customer. I mean, the client of the advertiser is the company for whom the product is being advertised.

But when this type of data collection occurs, it raises privacy issues of the Brandeis-Warren tort variety. And, in fact, claims that were brought in State courts against companies like Double-Click, and I don't mean to single them out because there were others as well, were based on the theory that you are talking about now, that you have this type of collection of information; a use that occurs; arguably, a form of unjust enrichment; I have seen that alleged—without a preexisting relationship.

Now, I think, a) this is a serious privacy issue, but b) the better approach, rather than going back and forth with a privacy tort state-by-state, is a general privacy law for this activity based on fair information practices that makes more open, more transparent when that data collection is occurring, makes it fairer.

Mr. BUYER. May I ask, Professor Feldblum——

Ms. FELDBLUM. Yes?

Mr. BUYER. [continuing] do you believe it is possible absent, in torts privacy, to have an inferred privacy cause of action?

Ms. FELDBLUM. I think it is very hard to imagine an inferred privacy without some contractual engagement at some point. I think where you are going to find——

Mr. BUYER. I am trying to find the boundaries. That is why I asked the question.

Ms. FELDBLUM. I think that where the differences will be is how far we are willing to see that contract extend; that is, somebody might say here is the contract and then that is it, and I think I would be someone who might say yes, that is the initial contract, but actually, there are other ramifications from that contract in terms of other people they interconnect with, and therefore, then, we get a privacy issue.

And that is when the context of the area makes a difference. It might be a difference if it is medical privacy, and they are interconnected there versus that I shop at Books a Lot. I mean, and that is a policy question, then, for you guys to decide.

Mr. BUYER. Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

Mr. Doyle?

Mr. DOYLE. Thank you, Mr. Chairman.

Professor Volokh, you seem to get a lot of questions. I am not an attorney, so bear with me. I want to make sure I got this right. My desire to keep certain factual information about myself private violates your First Amendment right to speak about me. Did I get that right?

Mr. VOLOKH. Not quite. Let me offer a friendly amendment. The government stepping in and suppressing people's speech to effectuate your desire, that would violate their speech rights. If the government goes and, as Professor Feldblum suggested, and tells a newspaper you may not publish this story, because it conflicts with the subject's desire to keep the information private, then, indeed, that is the government restraining the freedom of speech and of the press.

Mr. DOYLE. I have got you. So it is not inquiring minds have a First Amendment right to know; it is inquiring minds want to know. You are not saying that my desire to keep certain things private about myself violates your First Amendment rights.

Mr. VOLOKH. Oh, no, absolutely. If you are just doing it through technological self-help or through contract or through not revealing certain information, that is perfectly right. It is when the government steps in and tries to enforce that through coercive sanctions; that raises First Amendment questions.

Mr. DOYLE. Got you.

Professor Cate, you were not serious about that beer and diaper thing, were you?

Mr. CATE. Yes, I was.

Mr. DOYLE. That is incredible.

Mr. Rotenberg, that is all I have.

Mr. DOYLE. Let me ask you a question. We have talked a little bit about, you know, back in 1996 that companies started this self-regulatory approach to privacy, and here we are 5 years later, and FTC has basically come on the side that maybe the self-regulation hasn't progressed as much as it should. In your view, do you think the private sector has made a legitimate effort, a good faith effort to institute standards of behavior, or do you think they could be doing a better job?

Mr. ROTENBERG. Well, I think both statements are true. In other words, I think they have made a good faith effort. I think there has been progress. But I also think they could be doing a better job.

What I tried to do in my testimony, because this is obviously an area that you are going to come back to, I think, how well does self-regulation work, is to suggest a few issues you might want to consider.

Now, one thing that concerns me about this process of self-regulation is what I see as a redefinition of privacy. you know, we may sort of disagree about where the privacy rules apply, but I do not think there would be broad disagreement about fair information practices. That basic set of principles that can be found in a lot of places in U.S. law has been shortened, and today, we talk a lot about notice and choice, I mean, as a formulation for self-regulation. I think that is a very significant change in how we talk about privacy protection.

Mr. DOYLE. Thank you.

Professor Feldblum, you know, when we talk about commercial matters, I am not near as troubled as when we talk about medical matters, and again, I am trying to understand the legal issues. I mean, there is an implied privacy between a patient and their doctor that when you are sitting down discussing your medical situations with your doctor, you have a right to expect that that is not going to become public information.

Yet, I know—I live in Pittsburgh—the University of Pittsburgh Medical Center is undertaking this effort through this new technology project to be able to share information not only with doctors in their system but outside the system, so that when you go to a doctor, instead of waiting for film to be sent over and records that, you know, they can plug right into what standard, a system that can pull up all of that information.

But in the medical community, isn't this always done with some sort of waiver release? In other words, can my records actually be accessed by someone without me signing a medical waiver saying I give permission to send my records somewhere?

Ms. FELDBLUM. Oh, absolutely. I mean, that is what happens all the time right now. You will get——

Mr. DOYLE. Doesn't that seem——

Ms. FELDBLUM. Doesn't that seem odd? Well, you do sign waivers for things like payment and sometimes research. But, you see, what the medical community will say to you, and I think there is some value to this. One of the pluses about negotiating is hopefully, you learn and understand the other side is that they need some of that free flow of information. And if it was simply dependent on the consumer, the patient, agreeing, you would have too many people opting out, and then, that would hurt the quality of the system. That would hurt the quality of the information.

Mr. DOYLE. Give me an example of why they need the free—like, for instance, if I want to apply for a life insurance policy, I give a medical waiver saying, you know, check my medical records to make sure I am not going to die tomorrow. But I am saying give me an example of how stopping the free flow of information between doctors that I have not given any permission to do is a benefit——

Ms. FELDBLUM. Right.

Mr. DOYLE. [continuing] to consumers and/or the hospital.

Ms. FELDBLUM. The point, the idea is that the way research and quality and disease management work the best is by bringing in a lot of information. I think it was Congresswoman DeGette's point that sometimes, greater information actually helps the consumer, and the medical industry will say you may not realize that if you allow your medical information to be used, you will be helped with your diabetes as well, and you might not be smart enough now in the moment to realize you should give up that information.

So I believe, and my work in this area has made me believe, that we have to make sure that privacy regulation is workable for the industry, but that does include, No. 1, making sure that patients know where that information is going and that they do sign. Now, that is a sort of compelled consent, because if they don't sign, they don't get treated. But at least there is some information being given to them and that in areas where the industry can prove, look,

we need this information; we need it under the compelled consent, it has to be under a separate consent where if I don't sign, you can't refuse to treat me.

And to be honest, that is what the HIPAA regulations have essentially done.

Mr. DOYLE. Thank you.

Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

Mr. Shimkus?

Mr. SHIMKUS. Thank you. I think this is a family show, and I don't think I want to be effectuating my desire, as was stated. That was supposed to be funny.

I guess it didn't work. I am not a lawyer either, and I don't even pretend to be one.

And I am going to take this question, but I really enjoyed it. Let me state that. And I think it has caused a lot of questions. My opening statement said how do you balance? There are a lot of benefits to the consumers for trading of information, but there will be benefits to the business to keep the individual's records also.

In another subcommittee that Chairman Upton chairs, we are addressing the Webpages, domain names, and my personal interest is a move, if possible, to a .xxx domain name for that type of material, trying to address how do we skip away from the First Amendment debate on the people being able to go to those areas and for people to reap benefits from the publication of that smut, as a lot of us will characterize it, while protecting our children?

And with a .xxx domain name, filtering and technology could better support that, but you are not, in essence, infringing, I don't think. So I want to pose that to those who want to respond. I know Professor Volokh is ready to respond to that. What do you think are the First Amendment consequences? And then, it would translate into privacy because of the cookie issue and the tracking and all the other events.

Mr. VOLOKH. Just by sheer accident, it turns out that this is also an area that I have studied.

Mr. SHIMKUS. I knew that.

Mr. VOLOKH. But the Supreme Court, in Reno v. ACLU, said that the Government has very limited power controlling information online, even if it is sexually explicit information. Outside of the narrow zone of obscenity and child pornography, that speech is Constitutionally protected.

One of the things that the Supreme Court highlighted is there is filtering technology that parents can use to shield their children at home. I have argued that the Court may have overstated the utility of that technology; that the filtering technology is not perfect, and I think it is very important to realize that it is not perfect and never will be perfect. But it is probably the best solution, both from a Constitutional perspective—it may be the only Constitutionally available solution for parents, essentially, to use this technology and perhaps for the government to facilitate its development if necessary.

But what is more, as a technical matter, given the amount of offshore sexually explicit material which we might like to control, but we can't really, filtering is a necessary requirement, because fil-

tering is the only—the technological option is the only mechanism for controlling all the access that your child might have, whether domestic or foreign, because, of course, on the Internet, nobody can tell if it is domestic or foreign.

So I think filtering, with all its flaws, is the best solution both technically, practically and Constitutionally.

Mr. SHIMKUS. Following up on the actual—the ICAN, which is a pseudo-government entity——

Mr. VOLOKH. Yes.

Mr. SHIMKUS. [continuing] that assigns domain names——

Mr. VOLOKH. Yes.

Mr. SHIMKUS. [continuing] what about their requiring—two issues: requiring pushing sexually explicit sites into a specific domain name, and then, there is, again, would be copyright issues as far as forcing them from their name of choice that they have been using and everybody has familiarity with to another domain?

Mr. VOLOKH. You know, I am not an ICAN expert, but while I understand that there is talk, excuse me, of the .xxx suffix——

Mr. SHIMKUS. Yes, we had a hearing on that.

Mr. VOLOKH. Yes.

Mr. SHIMKUS. And it didn't go as well as I would have liked.

Mr. VOLOKH. I think while ICAN can set up that system, I think it becomes much harder for ICAN, then, to say and, by the way, you can't have sexually explicit material on any other things. So it is one thing for them to create a special domain name. It is another thing for them to start policing what is going to happen on other domain names. Even setting aside the legal question that happens if they say oh, we are going to revoke your .com address because we find pornography on your site, there is a whole host of practical questions: how are they going to figure out what is on your site? How are they going to hold a trial on whether it is sexually explicit? What happens if you have links from your site to some other site with links to .xxx?

So while I think this might be a channeling mechanism by which the job of filter providers could be made easier, because it would be a win-win-win for everybody, I don't think it would work as a coercive mechanism.

Mr. SHIMKUS. Mr. Rotenberg?

Mr. ROTENBERG. Yes; well, let me just say we participated in the Communications Decency Act litigation. We have also looked at the filtering issue. In fact, we have a publication called Filters and Freedom that looks at the strengths and weaknesses. But I very much agree with Gene on this. I mean, I think you can set out the domain and try to encourage its voluntary use, which would be beneficial, but at the point that you tried to, in effect, cordon off speech and say that certain speech, by government regulation, can only occur on certain places of the Internet, I think that would be very problematic and probably not permissible.

Mr. SHIMKUS. My time is up. I yield back to you, Mr. Chairman.

Mr. STEARNS. I thank my colleague.

Mr. Terry?

Mr. TERRY. Thank you, Mr. Chairman.

This has really been a——

Mr. STEARNS. Mr. Terry, let me go to this side and pick up Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

This has been an interesting and a diverse panel, as it should be.

To sum up what you have talked a long time about probably isn't completely fair to you, but, you know, anyway, let me just sort of, if I could, lay out what I see as sort of some parameters here. I guess it is Dr. Volokh. Basically, it seems to me you are saying that you don't have a right to stop or I don't have a right to stop someone from talking about me once it's out in the public domain, but it would seem that, as an individual, you know, we have the right to pull our blinds at night. We have the right to close the door.

Mr. VOLOKH. Absolutely.

Mr. GORDON. We have the right to, under certain circumstances, have our divorce sealed. We have the right to, in contracting with someone in a business deal, saying that if you divulge this information, then the business deal is null and void.

And, Ms. Singleton, you say that to think that to own the right to control information about yourself is a radical thought. It would seem to me that it would be radical to think that you can't, but again, that is where you are, it would seem.

And then, Dr. Feldblum is more pragmatic in that, you know, let's take things, as you say, in context. We will figure them out as we go along.

Now, as legislators, you know, I am trying to find out what our field of play is. We can doing nothing, or we can do, obviously, something. Now, getting outside of the realm of what you think ought to be done—that is our decision—what I am interested in knowing is how far we can go. You know, what is our outside limit? We know that our outside limit on doing nothing is doing nothing. Now, our outside limit on doing something is what I would like to find out. Whether we go that far is another matter.

So why don't we start with the three individuals I just mentioned, and hopefully, we will have time to talk to others in trying to succinctly tell us if we chose to go forward with legislation, how far could we go, in your opinion, Constitutionally?

Mr. VOLOKH. Sure. One is disclosure requirements. Again, this is what you could do. There may be some practical problems with it, but you could require that sites reveal their privacy policy. Another thing that you could do is that you could set up default contractual terms that are waiveable by the site, but they would have to be waived in a very explicit way that is evident to people. So, say, there are certain kinds of transactions where the default assumption that people engage in is no, you are not going to reveal—you are not going to pass along these photographs that I send you.

And if that is so, then, if you want to have a different rule, Website operator, you have got to make it absolutely clear that the users know and have an option not to do business with you.

A third thing is—and here, I agree with Professor Rotenberg—there are certain kinds of surreptitious data gathering. An extreme example would be them planting a virus on your computer or having them collect data in a situation where there is really absolutely no reason to think that there is any data being collected. Those kinds of data gathering restrictions, I think, would be permissible,

because they are not focusing on disclosure. They are more like saying no, you cannot peek into my windows using a telescope.

So, requirements that a site disclose its policies; setting up default provisions in the contract that will be enforced unless the provisions are disclaimed; and restrictions on certain kinds of surreptitious data gathering.

Mr. GORDON. That's for preventive measures, though.

Mr. VOLOKH. Pardon?

Mr. GORDON. Preventive measures up front is what you are——

Mr. VOLOKH. Yes, yes, exactly.

Mr. GORDON. And, Ms. Singleton, it is sort of Katy, bar the door with you. Are there any limits? Is there any action that you think that we could take legally, whether it was good policy or not, but it was legal?

Ms. SINGLETON. I would say generally, from a Constitutional standpoint, the more targeted the legislation is to a specific, identifiable harm, such as identity fraud, the more likely it is to pass Constitutional muster. The further you move toward sort of omnibus rules that are applying even in situations where there has not necessarily been any harm to consumers that has been identified, that might be a different story, but a lot of it depends on the details of the legislation, the costs it imposes on industry, and a lot of those, frankly, are unknowns at this point.

Mr. GORDON. So is there a Constitutional right not to have costly measures placed on you?

Ms. SINGLETON. The question in the free speech case as it comes up is how much of a burden is it on the dissemination of truthful information? Are you restricting——

Mr. GORDON. So why should cost be a matter? It should be, maybe, a policy matter, and I think it should be, but why should it be a Constitutional matter?

Ms. SINGLETON. I guess because cost is part of the picture in terms of what the impact will be on speech. Will there be, essentially, chunks of speech that for cost reasons no longer are permitted to exist or move around, even though there is no particular harm being done by those bits of speech?

Mr. GORDON. Okay.

Ms. SINGLETON. I hope that answers it.

Ms. FELDBLUM. I would say to the three areas that Eugene noted would be Constitutionally allowable, I would add three others. One that I think you can put prohibitions on further redisclosure, even with someone whom you are not in that direct contractual relationship with, and that is part of what we have talked about.

Two, I think in some situations, I don't think we should allow that default contractual rule to be waived. And the medical profession, I think, is a classic example, because of the need and power, sort of, situation, and I am not sure what I would think in terms of other commercial settings, but I would not do it as an absolute rule that that can be waived, that default contractual obligation for confidentiality.

And three, besides the mandated disclosure, I think in certain areas, an informed consent is, in fact, Constitutionally appropriate as well. Again, I think that fits well in the medical arena. Whether

that also fits in as a required opt-in in a commercial, I think, is more of a policy question.

Mr. GORDON. The benevolence of the Chairman may allow you to talk some more to other candidates, but in case he doesn't, I would like to ask that each of you submit to the committee a written statement as to what you think are the Constitutional furtherest bounds that we could go in legislating. If you want to add to that why you think maybe we shouldn't, then, that is fine. But I would like to find out what the field of play is, and then, hopefully, ultimately, we can maybe find some common denominators.

Mr. STEARNS. The time of the gentleman has expired.

Is that acceptable, doable, feasible for you folks to do that. I think it would be very helpful for the committee.

Mr. Terry?

Mr. TERRY. Thank you, Mr. Chairman.

I think all of our questions here are focused on trying to find that boundary or at least the lowest common denominator of what should be done, what could we do Constitutionally, legally, without restraining trade.

Let me work some of that. Can I have an hour? Since I am the last to ask questions?

Mr. STEARNS. Will that do it?

Mr. TERRY. I will try and do it within the 4½ minutes that are left.

Mr. STEARNS. I would say to the gentleman we are going to do a second round.

Mr. TERRY. Okay.

Mr. STEARNS. I think, with the panel's indulgence, there are not that many members, so we are going to do a quick second round which would be an additional 10 or 15 minutes.

Mr. TERRY. I think one of the areas I would like to explore, but I am going to try and discourage, is it seems to me that perhaps there should be a sliding scale. Of course, we want higher protections on sensitive material like medical information, but yet, should commercial information about my buying habits of diapers and beer have this same heightened scrutiny and protection? And I would probably say right here without exploring it more that no, there should be probably a laxer standard on my purchase of Bud Light and Pampers. And by the way, more young people drink beer, and more young people have small children in diapers: case in point.

And so, let's go with that. Mr. Cate, I want to explore some of these boundaries of when there should be some rules protecting commercial information in place, and I am going to kind of give examples of how that information can be, then, redisclosed throughout the system and see if maybe higher standards should be put in place as the information is disseminated.

Let's say I go to the grocery store, and I use my credit card. It is issued by my bank. And, Professor, let's say, for example, you in answering this question, and I want your personal opinion, are my bank and the credit card issuer. Is it appropriate for you, then, to have software that would be able to read that when I use my credit card or my debit card to purchase at the grocery store that I buy Pampers and Bud Light? Is that appropriate that you even

have that technical ability? And should I, as a consumer, when I sign up for my credit card, know that you may have software where you are going to know that I am specifically buying that brand or diapers generically but that brand specifically? Is that appropriate?

Mr. CATE. Yes, it is appropriate.

Mr. TERRY. Should there be laws in place that I know that that is occurring?

Mr. STEARNS. Mr. CATE. It is appropriate that it occurs, and it is appropriate that you should know.

Mr. TERRY. All right; is it appropriate that perhaps Congress adopts some policy and law that mandates it on Professor Cate Bank and Credit Card Company?

Mr. CATE. Well, let me say the answer to that is yes but, and if I can just have, you know, 5 seconds to say the but, which is you can send out all the notices in the world to customers, and they will throw them away with enormous glee. And so, if the effect of that notice is simply to impose a $1 billion cost—although it does subsidize the Post Office, which is not an unimportant issue—but not to educate the public, then, I think that it is not advisable, although it is clearly legally permissible.

Mr. TERRY. And I will tell you right now: I want to make sure that when I open up my credit card bill that I don't have a bunch of trashy coupons in there. Give me a Pampers coupon, because I am spending a heck of a lot of money on diapers. So I want you to be able to target it to me.

Now, let's say Professor Volokh is actually—you are just the shell. You just issue the darn card to me. You hire a separate business to actually do all of the contracting. Should he have the right, that company that is not you but your contracting agent, have that power, the software, the technology to be able to gather my specific buying needs, although my contract is with you?

Mr. CATE. I believe that he should.

Mr. TERRY. And either two of you, you can now expand on it.

Mr. CATE. But he can speak for himself now.

Mr. VOLOKH. Well, it seems to me that if the Cate Bank makes this promise to you that they are, let's say, not going to reveal it further or some such, then, they had better ask me to make the same promise to them, because otherwise, they might be liable to you.

Mr. TERRY. Should I know that you are part of that process up front?

Mr. VOLOKH. Well, it is an interesting question, because I think for most consumers, the exact financial structure or the exact business structure is not terribly relevant. I think with most consumers, my guess is—and here, you are reaching policy rather than Constitutional law—I think what consumers would like to know is what purposes their information is going to be used for. And it seems to me that——

Mr. TERRY. And that is the point I am getting to, actually, because if it just keeps coming back to me that since you are the one who is really going to send me out my bill with the coupons in it, because you have hired another company that actually prints and does all of that, which is the real world, if it keeps coming back to me, is there a lower standard than that?

Mr. VOLOKH. A lower standard?

Mr. TERRY. Of privacy and regulation, maybe just an opt-out type of policy instead of an opt-in type of policy.

Mr. VOLOKH. I would think that——

Mr. TERRY. Or just basic disclosure?

Mr. VOLOKH. I think there is a lot, especially given how much consumers are concerned about business, and it is interesting you mention credit cards. It is a very competitive business. A lot of people want your credit card business.

Mr. TERRY. And this is a lot of——

Mr. VOLOKH. Exactly.

Mr. TERRY. [continuing] when we get feedback from the business world on rights of privacy, it is usually in the——

Mr. VOLOKH. Yes; I would think that there are a lot of banks that would have a lot of incentive to say we are going to give you a high-privacy credit card, and we are going to promise that we are going to give you privacy; we are going to promise that we are going to use the information only for these very limited purposes. We are going to make all of our contractors promise the same thing to us, so that we can hold them to this obligation, too.

So it seems to me that the business world may do a good enough job if it is. If it does not, then, I think you could impose requirements that credit card companies facilitate consumer shopping by making it clear to the consumers what their privacy policies are.

Mr. TERRY. But I am running out of time, but the next phase of that would be selling my name to Anheuser Busch or whoever owns Pampers.

Mr. VOLOKH. I thought you had an hour.

Mr. TERRY. What is that?

Mr. VOLOKH. Well, I think if we promised——

Mr. TERRY. And I think that is what a lot of people are worried about.

Mr. VOLOKH. Yes.

Mr. TERRY. But with the consumer, heck, if I get something at a discount from Pampers——

Mr. VOLOKH. Yes.

Mr. TERRY. [continuing] I like that idea. But where do we draw the line in the process?

Mr. VOLOKH. It seems to me that providing disclosure of what is going to happen and thus providing meaningful consumer choice will allow consumers to decide: do they want the high-privacy, no-coupons, I just want to be as sheltered as possible credit card? Or do they want the go ahead; I don't care if people know I am buying the beer, especially if they want to send me more coupons? It seems to me that disclosure does provide consumers with more choice.

Mr. TERRY. I appreciate that, Mr. Chairman.

Mr. STEARNS. The gentleman from Massachusetts, Mr. Markey?

Mr. MARKEY. I thank the gentleman very much.

See, the point is that most people would not care if anyone found out that you were buying Pampers for your children. But your mother would care if you found out that she was buying Pampers for herself, Okay? That is a much more sensitive issue, very sensitive, incontinence pads for 2 million elderly women. They haven't

told their daughters. That is a different issue. So, yes, you don't care maybe necessarily.

But on the other hand, your mother is very sensitive about that. Only her husband knows; no one else, her sisters, her children. So what are we going to do for her? What rights does she have?

So, I want to give her a lot of rights, to be honest with you, because she built the country. She doesn't want that information disclosed; she has a right to keep it private. So I am very respectful of her; very embarrassed, because it goes right to her dignity, her pride. She can't control herself.

So where are those lists, and how do we get names off those lists? How hard is it to get your names off those lists?

So, we kind of have this duality, you know. On the one hand, you have got the industry coming before this committee saying we need more copyright protection for all of their information. Don't let anyone disclose it. It would be terrible if anyone ever took our information and sold it, you know. Look at Napster. That Napster is going to ruin us, you know. We listen attentively.

Then, the individual says, oh, by the way, I want a copyright on my own personality, my own information. You can't do that, says the very same industry. You are not entitled to copyright your information. That is different, Okay? But don't let them take mine.

The industry comes in here, and they say you have got to have the top-notch, No. 1 encryption technology available to every consumer, security all the way, all the way from your house to my bank, my Internet company. Security, very important. But once I get the information, you shouldn't have any privacy. Now, from a consumer's perspective, they say, well, I do support state-of-the-art encryption, because I don't want the kid across the street cracking in and finding out what I am doing. But I don't want you to do it either. I am only transacting, you know, for this one little deal.

So there is a duality here. The industry says copyright good, security good; privacy bad, privacy bad. But we need the same high standards, because from the consumer's perspective, they see the same issues, okay, that the industry does. And the paradox is quite obvious. So begin, then, Professor Volokh, you begin with the question of your children. Did we make a good decision in passing the Children's Online Privacy Act here, saying that parents have to be consulted whenever any information on a commercial site has been gathered about a child under the age of 13 that could be reused for purposes other than that which the parent intended? Do you think that was a good law, first, to pass, Professor?

Mr. VOLOKH. I actually have no opinion specifically on that law, because I think that the situation with children revealing information, because children are incapable of consenting, is actually a much more difficult question.

Mr. MARKEY. No, what I am saying is what is your view then? Is that a good law for us to pass?

Mr. VOLOKH. Believe it or not, actually, I don't have an opinion, and in my article, I actually specifically say it is an interesting question that I haven't examined.

Mr. MARKEY. No, I don't believe you don't have an opinion. I mean, otherwise, you shouldn't have been invited, to be honest with you, Okay? Because that is too simple a question, to be honest

with you, okay, for somebody who his holding himself out as an expert. What about children under the age of 13, Professor? Should parents have to give their approval if a commercial Website is going to reuse the information for purposes other than that which the parents intended?

Mr. VOLOKH. I believe I wasn't—I'm sorry.

Mr. STEARNS. Professor, hold on. Just a comment.

Mr. VOLOKH. Yes.

Mr. STEARNS. I would say to the gentleman from Massachusetts we asked these people to come here for their legal interpretation and not necessarily for their personal interpretation, for what it is worth.

Mr. MARKEY. I appreciate that, but, Professor, that is hard, because they have rapt audiences in law school that hear both their legal and personal opinions, and so, they are usually packaged almost in a way that is so intertwined that it is impossible to really separate them as a student, okay, but as a Congressman, I am in a position—Father Drinan was my dean in law school. And then, in my second year, he wins for Congress. So I was so intimidated by him. But then, 6 years later, I got to be a Congressman, too. And so, whenever he voted yes, I could vote no, you know, if you know what I mean, okay?

And I have to admit: it was gratifying, although in retrospect, he was probably right on everything.

But at least I was able to question more, you know, intensively any position which he had.

So all I am asking, Professor, quite simply is would you personally, as you hear the question, give that child audience more protection?

Mr. VOLOKH. Representative, I was invited here, I thought, to comment on those matters that I thought I was competent to comment on. In my article, I specifically said that this is an issue that is very tough that I have not spent the time necessary to think about it, because whenever children are involved, especially with questions of consent, that raises all sorts of difficult questions. It seems to me the only responsible thing for me to say is to admit that I have not thought about this enough to have formed an opinion.

Mr. MARKEY. Okay; well, let me just say that—okay, you can play that.

My view—I will say my view. I think children should be protected, and it came out unanimously out of this committee, and I don't think you are going to get much dissent across this country. You may be the only person in the country without a view on that issue.

Really, but that is okay. I mean, I don't mind that you want to take that position, because of course, that immediately begs the question of whether or not 14-year-olds should be protected, okay? You don't have to have a view on that, either, but I would say yes, 14-year-olds should also be protected. We didn't do that. We only did it up to 13. And then, how about 16-year-olds? And I would say 16 years old as well, okay? Looking at it from a societal perspective, you know, that they should be protected.

And then, you just keep going. You keep asking the same question over and over again, okay? And that is what we do as a matter of public policy. But you can start from one perspective and say okay, on the one hand, you know, maybe this information should be out there free and, you know, unrestricted. But then, if you take it from the other perspective, you are saying no, it should be restricted, because you have got this special category down here, and then, you have to decide how far up you are going to take the special category, which is the much tougher question, because it doesn't fit into a uniform philosophy. And, of course, that is the most valuable information to us: what doesn't fit into a uniform philosophy?

Mr. STEARNS. I would tell my colleague we are going to do a second round.

Mr. MARKEY. Excellent. I am ready. Excellent.

Mr. STEARNS. I am going to start and ask Ms. Singleton: emergence and diffusion of certain new technologies, such as the Internet, have triggered today's debate on information privacy. Would you please place the relationship between new technologies and privacy debates in historical perspective?

Ms. SINGLETON. Yes; let me do this very quickly. One of the interesting things that began to happen in the early Twentieth Century is that credit reporting became professionalized. It was originally done sort of as a nonprofit activity to help poor people get access to credit, and today, it has become professionalized and become, you know, a professional thing.

Now, this goes to my point that privacy legislation, even relatively minimal opt-out, is not nearly as moderate as it appears on the surface, because if there had been an opt-out rule in place during the period of time in which credit reporting was developed, there simply would not be credit reporting. All of the people with bad debts would simply have opted out.

To move up to another example today involving the Internet, just a few years ago, identification and authentication became a very important function that e-commerce companies needed to have. Amazon.com, for example, when they get an order from a customer, they check the name and address against a massive commercial data base with pretty much everyone's name and address in it and absolute as updated and accurate is possibly can be.

And if people were allowed to opt out of this data base, its value as a commercial enterprise, once it was full of holes and gaps and so on, people opting out, whether for well-meaning purposes or because they want to conceal who they are, would essentially make this authentication and identification much less useful.

So I think there again, as we think about the evolution of technology, it is important to realize that there are uses of information that are very innovative that haven't been thought of yet, some of which could turn out to be tremendously beneficial to consumers and which even relatively moderate legislation might foreclose.

Mr. STEARNS. Mr. Rubin, Professor Rubin, in your study, you identified no market failures. Do market failures primarily result from information asymmetry? And if so, how does information sharing relate to market failure?

Mr. RUBIN. Information asymmetry is one——

Mr. STEARNS. You might define a couple of terms.

Mr. RUBIN. Information asymmetry is when one party knows something, and the other party does not know it, but as it is used in economics, which is my field, by the way; I am the only non-attorney here, I think—as it is used in economics, it means that people are, in those circumstances, less willing to transact. So if I know there is an information asymmetry, I may be unwilling to transact.

But the way to solve information asymmetries is to create more information. And so, the free flow of information actually is likely to solve problems of information asymmetry.

Now, with respect to the Internet, you might argue that in the early days of the Internet, when people did not understand data collection and didn't understand that information was being collected, there may have been more of a problem. But now, all of the surveys show that people are fully aware of the fact that data is collected. This creates an incentive for Websites to post privacy policies, for example, and tell people how the information is being used, which creates an incentive to eliminate the information asymmetry because it makes people more willing to engage in transactions.

And so, in a sense, the market is solving that problem by the posting of privacy policies, and the FTC study showed, for example, that 100 percent of the most commonly visited Websites did post privacy policies, not because they have been mandated to but because it is in their own interest to do so. So in a sense, the market has been solving that problem.

Mr. STEARNS. But the problem is you go to some of these sites, and the privacy request is way down, and you have to scroll all the way down. And then, it is a light gray line. And then, they put another light overtone on the light gray line. And so, you have got to see that, and you have got to double-click on the privacy. Then, up it comes, the dialog box.

So, I mean, they are volunteering, but they are volunteering in a rather clever way or a way that is an obtrusive, so that the average person doesn't even know that they have a privacy policy.

Mr. RUBIN. But if people want privacy policies, a natural reaction when you go to a site where you can't find it is to simply leave that site, to assume that it doesn't have one, or it's not worth my looking for it. If people are concerned about privacy policies, then sites have incentives to make them available and to make them more easily available, because otherwise, they are going to lose consumers.

Ms. DEGETTE. Will the gentleman yield?

Mr. STEARNS. I will yield.

Ms. DEGETTE. But what if they don't see the privacy disclaimer, so they just assume that privacy is included? Isn't that also a possibility?

Mr. RUBIN. Well, I think it is less of a possibility now, because as I say, the surveys show that people are concerned about privacy. I don't think people have an expectation that the default is they are going to protect privacy.

Ms. DEGETTE. Has there been research done on that?

Mr. RUBIN. I haven't seen specific research, but there are all of the surveys that do show people concerned about privacy, which means yes, I guess that would indicate that people don't expect information to be kept private without a disclaimer, because they are concerned about the way Websites use information.

Mr. STEARNS. Let me just indulge myself with one other question for you. Please define the free rider problem and explain its relevance to the information privacy debate. Explain what you mean by free rider problem.

Mr. RUBIN. Free rider problem is where someone can benefit from something without contributing. So, for example, if information, collecting lots of information, is valuable for the credit reasons and the other reasons that we have talked about, so that creating lots of information can create a marketplace, but I, myself, would prefer to benefit from that marketplace and not contribute that information, then, I would be what is considered a free rider.

So I might say it is good if Websites can make these determinations, but I don't want to tell them my information. I am going to benefit from the things that are provided without contributing; then, that would be a free rider, and under certain circumstances, you would have a free rider problem in the provision of such information.

Mr. STEARNS. Okay; my time has expired.

Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman.

To follow up, Professor Rubin, I think that to make the studies more pedagogically sound, it might be interesting to research consumer attitudes when they don't see a privacy disclaimer, because I would opine, based on nothing except for common sense, that people going into certain types of sites—financial sites or where they are going to be disclosing personal information—may well still assume that there would be some privacy given, for example, similar to when they went to the doctor, and there is not, on your regular medical form, a privacy disclosure, but yet, people assume that their doctors will keep their medical records private.

So I think that would be some useful research to conduct, and I would hope that it is being done.

Mr. Cate, I have a couple of questions for you. I wanted you to expand a little bit on your written testimony where you talk about how requiring a customer's consent exacerbates the harmful impact of many privacy laws on consumers. How do you see that happening?

Mr. CATE. Well, I provide seven or eight examples in the testimony.

Ms. DEGETTE. Right.

Mr. CATE. So let me just touch on a few of those——

Ms. DEGETTE. Thank you.

Mr. CATE. [continuing] and try to make them clearer.

One of them, of course, is if consent requires repeated contacts or requests to the consumer. So, for example, even under the Gramm-Leach-Bliley law, the average American household gets 20, 30, 40 notices. That is with a cost that is paid for by consumers. That is an environmental burden that is borne by all of us as citizens, and it is a burden for people who say they don't like the junk

mail they get already; they are now getting more junk mail mandated by Congress. So that is a clear burden on consumers that the opportunity for consent, the mandated opportunity for consent, exacerbates.

I think, for example, in the health privacy rules that are out now, we see even more of that. That is where, for example, the length of that notice, the fact that notice will be interposed between the patient and the physician at every occasion; I mean, even the mundane question, you know, I go to the pharmacy to pick up a prescription for my wife, but, of course, I can't do that under those HIPAA rules, because only she can consent, and her consent is required by regulation for her to receive that prescription.

So, now, she has got to go to the pharmacy to pick up that prescription and sign that form first. I think that is a real burden.

Ms. DEGETTE. What is your view on that, Professor Feldblum?

Ms. FELDBLUM. My view is that sometimes, Professor Volokh's approach of not talking when you don't know it all the way through is a good one. The HIPAA regulations specifically dealt with that and, in fact, have set it up so that other people can go to the pharmacy to pick up.

Ms. DEGETTE. How will that work under the HIPAA rules?

Ms. FELDBLUM. Because there isn't the ongoing consent each time. You consent for that information to go for certain purposes, and you consent for other people to do that on your behalf.

Ms. DEGETTE. So you think his wife would be able to go pick up that prescription?

Ms. FELDBLUM. Absolutely, absolutely.

Mr. CATE. Not the first time.

Ms. FELDBLUM. I completely stand by that.

Ms. DEGETTE. Not the first time, but subsequently after she signed the thing?

Mr. CATE. Absolutely; that is right.

Ms. DEGETTE. But you think that is an undue burden?

Mr. CATE. I think that is an example of a burden.

Ms. DEGETTE. Okay.

Ms. FELDBLUM. And to your question of the expectations of privacy, you are right. People think when they go to the doctor that that information is going to be kept private. And, in fact, until we have these regulations effective, they, in fact, don't really know where that information is going. So the problem we currently have in the medical system is also the problem that exists in your question about some of those sites. People don't know enough, and as Eugene Volokh said, the one thing Congress can do without any concerns is mandating some more clear disclosure. And that is, in fact, what the HIPAA regs do.

Ms. DEGETTE. Let me get back, Professor, for a minute to the H.R. 10 privacy restrictions. Is it your view that under that law that that law requires repeated notices to customers? Because as I say, I was on that conference committee, and that was not my sense.

Mr. CATE. That law requires that those notices be delivered annually, yes.

Ms. DEGETTE. And you think that that is an undue burden?

Mr. CATE. There is no question, because, for example, there could be no use of information at all; you know, I am not making any third-party use; I am not distributing it to anyone; I am not marketing. Therefore, there is no opt-out right involved. There is nothing at all that the consumer can do based on this other than, of course, stop engaging in the service. And there can be no change in the information used from year to year. But still, that notice has to be sent out.

Ms. DEGETTE. Mr. Chairman, I just want to say that I think this was a great first start on this privacy question. We obviously had a breadth of opinions here, and I, myself, having sat through many law school classes where the professors grilled me—am very, very happy to have my little comeuppance. So thank you all for coming today.

Mr. STEARNS. Mr. Terry?

Mr. TERRY. Thank you.

I said earlier that I don't see a problem with having completely different standards for what we think as a traditional commercial transaction versus a medical transaction. Is that appropriate legally and public policy-wise in your opinions?

Ms. FELDBLUM. Well, two things: one, and I think it was sort of referenced by Representative Markey's comment: often, there is an integration of those in a way that can be complicated. So I think that while, as a conceptual matter, yes, there are different harms, given our system of credit and finances and educational institutions sort of being connected in with some medical information, it means that you have got to think through all of those elements.

The second is really more a matter of, you know, really what both Ms. Singleton and Professor Volokh have written about, which is the conceptual question of how much control should you have over your own information? And for people who feel that strongly, it really doesn't matter that much about whether it's that they're taking a particular medical drug or that they like to buy a certain type of, you know, videos, you know, even action videos.

You know, I am someone personally who I don't really—you know, I like getting coupons for things that I care about, right?

Mr. TERRY. Right.

Ms. FELDBLUM. On the other hand, if I am sitting and making policy for everybody, I think I need to think about what sort of control do I want to give these folks consistent with not messing up the commercial system? Because that is going to help everyone as well.

So, yes, there are differences, but there is integration of that information, and two, you have to legislate for the general public.

Mr. ROTENBERG. I think the problem is actually somewhat more complicated than this, and the reason is that when you are talking about a sectoral approach to privacy focusing on subject matter—I mean, we agree that medical information is more sensitive than commercial information—it puts aside the significance of technology. Now, consider, for example, the privacy protections associated with the use of the telephone system. You pick up the telephone, and you call up Safeway, and you say do you have any diapers left? You call up your doctor, and you say do I need to get that prescription refilled, because this problem is continuing.

The privacy protection that exists for your telephone call, whether you are calling Safeway about the diapers or your doctor about the prescription is the same. Now, it may be the case that if someone intercepts the call and discloses the fact that you were talking about diapers, it wouldn't be embarrassing, or it could be the case that even the medical information isn't embarrassing. But it is interesting that if you look at the development of privacy law, video rental tapes—probably most of the tapes that you rent, not that sensitive. But some may be. The law provides comprehensive protection across this new technology in which consumers operate, and I think it is very important to keep this in mind, because there is a tendency when thinking about privacy protection, and I think it is common sense to sort of distinguish and say, well, some things are very sensitive; some things are not. Let's focus on what is sensitive. It makes sense.

But when you talk about the integrated nature of technology that allows both sensitive and nonsensitive information to be exchanged, I think you need a more comprehensive approach, and that is why I would not recommend, actually, going based on subject matter in trying to define privacy.

Mr. TERRY. Let's continue, because I think there will be a variety of opinions. I respectfully disagree. I just don't see how you actually physically do it in the real world, because in order to treat everything equally, we have to move to the strictest standard, and I can't believe that I would have to sign a—I mean, literally, take a consent form to go to the grocery store and use my debit card. I mean, if we want to take that to the extreme that——

Mr. ROTENBERG. But I don't think you would.

Mr. TERRY. Well, it depends. If there may be something that, you know, if you move to the strictest standard, you would.

But let's keep going down the field, because we have got to explore the boundaries of what we can do.

Ms. SINGLETON. Yes; I think that there is one potential problem with sectoral legislation, and that is you may have a situation, as you have with Gramm-Leach-Bliley and the new medical privacy standards, where there are companies where their same data base is governed both by the Gramm-Leach-Bliley Act and by the new medical privacy rules, and those rules set a different legal standard.

So what does the company do there? In some cases, one standard may be higher than the other one, in which case you just comply with the higher standard. But in some other cases, it is not really that clear, and the standards are just different. So that is one problem, and I think the answer to that is when you do sectoral legislation to narrowly target that legislation at a specific, identifiable harm such as fraud.

Now, some people would say why don't we just have legislation all across the board to solve that problem? And my answer to that is because that is way too broad. Its impact on the economy would be enormous and very difficult to even grasp at this point. And plus, it also has a really big impact on small businesses potentially.

Mr. STEARNS. Do you want to make your—his time has expired. Do you want to make your comment short?

Mr. RUBIN. I will try to make them short.

I think there is a difference between information that starts with a person and says what do we know about Paul Rubin as opposed to most of the commercial information, which starts with a product and says how can we find Websites of consumers who are interested in buying this product? So medical information, much of it, would fit into the first category, and the sort of commercial information I am talking about fits into the second, and I think that may be a way to think about a differentiation.

Mr. STEARNS. Thank you. Time has expired.

Before I have my colleague from Massachusetts finish up our great hearing here, he mentioned Congressman Drinan. He came here, as I recollect, a professor from Georgetown.

Mr. MARKEY. No, from Boston College.

Ms. FELDBLUM. From Boston College. He is now a professor at Georgetown.

Mr. MARKEY. Downward social mobility.

Mr. STEARNS. And Mr. Markey mentioned how much reverence and awe he had of him, and I am reminded of an expression that we all know as Members of Congress: the first 6 months, we wonder how we got here. And then, the next 6 months, we wonder how the rest of them got here.

Mr. MARKEY. As he introduces me!

Mr. STEARNS. Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman, I appreciate it very much.

Not only that: Boston College is number 10 in the AP basketball ratings, and Georgetown is number 16, okay?

So it was the only small little area of advantage they maintained over us, and now, it is complete domination.

So we're quite happy—with the exception of their privacy division in the law school—and that one Constitutional law professor emeritus, you know, Father Drinan, they are the—so here's the way it is. And Professor Rubin said, you know, most of these sites now have a privacy policy, and they do post their privacy policy. We have a privacy policy, it says, okay?

Then, you read way down here. It says—by the way, after you have hired lawyers at $700 an hour to write a 14-paragraph privacy policy with double negatives just driven throughout the entire thing just so that they can prove they went to law school, and down here, after you get to the bottom line, they could have just said you have no privacy. We reserve the right, of course, to sell this stuff, okay? But it is their policy, though. It is their policy. And who the hell is going, you know, to read 10 paragraphs on every single site they go into?

So, obviously, that doesn't work. The free market—yes, they put it up, but it is like an attractive nuisance. It is misleading in a lot of ways, do you know what I am saying? You are sucking people in where they shouldn't be going, because they aren't going to go through all 10 paragraphs.

And the thing is, well, financial, of course. It is the financial. You know, you might have been writing the check for your kid's Ritalin or your kid's child psychiatrist on the checks for the last, you know, number of years. That is medical, okay? More sensitive; you don't want the whole neighborhood, you know. You promised your

daughter you are not going to tell anybody, you know, much less everybody in town can get it as a direct mail, you know, from the financial institution.

And the same thing is true for the medical exams, for the insurance, you know. That is also very sensible. So the financial oftentimes is nothing more than the genetic makeup of the family's medical history for the last 30 years, you know, just sitting here if you can go through the medical. So it is hard sometimes to tease it out, in other words. It is basically inextricably intertwined inside of those financial data.

And Citigroup, somehow or other, in Germany figures out how to do it, but they just can't figure out how to do it in the United States when these higher privacy standards are put on the books.

So let me go down with just a very quick question to each one of you. You basically disclosed what Federal contracts you might have. What private contracts do any of you have, any financial interests that you might have in your life apart from your law school careers that would influence to oppose the most stringent privacy policies? Can you tell me which companies, any consulting contracts that you have—we will go right down the line—with outside groups?

Mr. STEARNS. With the indulgence of my colleague, as I recollect, and, counsel, you can correct me if I am wrong, when they came here, did they fill out—was that our policy?

Mr. MARKEY. No, I have their forms. I have their forms right here. This only deals with their Federal contracts. It doesn't deal with their private sector contracts.

Mr. STEARNS. Well, what I am just saying is that what they filled out is all we requested from them.

Mr. MARKEY. Oh, they don't have to give this to me right now. I am asking them as a favor to tell me. It is just a question. They don't have to tell me.

Mr. STEARNS. So this is a voluntary——

Mr. MARKEY. Right.

Mr. STEARNS. [continuing] exercise here.

Mr. MARKEY. Right.

Mr. STEARNS. In which he is asking you to divulge personal information about your privacy.

Mr. MARKEY. Exactly. Now, you have got it. You have got my point.

Mr. STEARNS. He wants to know things about you personally.

Mr. MARKEY. I want to know things about them, you know.

Mr. STEARNS. So under his timeframe, you can say that it will take you awhile to get it——

Mr. MARKEY. Yes.

Mr. STEARNS. [continuing] and you will get back to him——

Mr. MARKEY. You can say that.

Mr. STEARNS. Or do whatever you like.

Mr. MARKEY. But I think that they all probably know where their income comes from each month, so can you tell us? Can you just go down the line, and then, you know, we can all hear?

Mr. CATE. Well, I am perfectly happy to answer your question if the question is what consulting contracts I have. I am senior counsel for information law to a law firm in Indianapolis by the name

of Ice, Miller, and that is the only ongoing consulting relationship that I have.

Mr. MARKEY. Do they have any clients that you are writing——

Mr. CATE. I am sure they have many clients.

Mr. MARKEY. [continuing] memos on at their request on this issue of privacy?

Mr. CATE. They do have clients that I work for, yes.

Mr. MARKEY. Can you list a couple of those clients?

Mr. CATE. I cannot list those publicly, I am afraid.

Mr. MARKEY. They like their privacy, don't they?

Mr. CATE. No, I think they protect the confidentiality of their relationship with their attorneys.

Mr. MARKEY. As I am saying, the public would call that privacy. The law firm has a different word for it.

Mr. STEARNS. If the chairman would just indulge, the gentleman from Massachusetts is an attorney, and isn't there a client privilege that——

Mr. MARKEY. That is exactly my point.

Mr. STEARNS. [continuing] you are trying to divulge here a client privilege?

Mr. MARKEY. That is exactly my point.

Mr. STEARNS. That is a contractual relationship that they have with their clients which they don't want to divulge, and so, I suspect that you are putting them on the spot here by doing that, which I know you are trying to make a point.

Mr. MARKEY. Well, we can go down, and we can just see how many times they want to invoke client-lawyer privilege, because this is not exactly national security here that you are writing memos on the privacy policy for private sector firms, okay? This is not something that I think we would put in the highest category. We would put this down on the lowest category: I am on espn.com finding out where BC is this week compared to Georgetown, okay? But the fact that private sector companies need privacy memos, okay, doesn't seem to me that it would be the highest level of privacy protection; not up there with medical and financial, for certain. I would put it in the lower category.

Mr. STEARNS. Well, the gentleman's time has expired. So, saved by the bell.

Mr. MARKEY. I don't think that's fair, Mr. Chairman.

Ms. DEGETTE. That is not right.

Mr. MARKEY. That is not fair to me. They should all have the right to say no, I don't want to tell you. I think I have the right to have a no.

Mr. STEARNS. I think the Chairman also has a right to say that time has expired when the member's time has expired.

Ms. DEGETTE. Mr. Chairman, I will ask unanimous consent to let these witnesses answer the question. You haven't cut any other member off today.

Mr. STEARNS. Well, no, but I think in a free discussion here I would say to my colleague that we have had an opportunity to understand Mr. Markey's point, and I don't necessarily want to take these witnesses who have come here, to ask them to divulge personal information.

Mr. MARKEY. I don't want them to. I want them to say no, I don't want to disclose it. Don't you understand? No, no, no, no, no, and then, I am happy. It is over. It will be under 10 seconds.

Ms. DEGETTE. Does that mean, Mr. Chairman, you are objecting to my unanimous consent request?

Mr. MARKEY. I don't want to tell you; I don't want to tell you; I don't want to tell you.

Mr. STEARNS. No, what I am saying is that even by them saying that they don't want to answer, that is putting them in a position which I don't think they should have to be put in, and that is my prerogative as the Chairman, and that is where I stand.

Mr. MARKEY. I don't think you can do that, Mr. Chairman. I really do believe that they have a right and the ability as law school professors to protect themselves. How about in writing? How about if you would each give it to me in writing? How about if I asked them all, because I can see the reluctance that is sitting down there. Nobody is raising up their hands saying I don't have a problem.

Mr. STEARNS. I think that is a very good compromise.

Mr. MARKEY. But if you send it in writing, I would very much appreciate it.

Mr. STEARNS. Okay.

Mr. MARKEY. Would all of you agree to send it in writing?

Mr. VOLOKH. I am sorry. Actually, because it was suggested that our failure to say anything is reluctance to that, I would be very happy to say: I have——

Mr. MARKEY. He doesn't want to let you.

Mr. VOLOKH. Fair enough if he forbids you from——

Mr. STEARNS. His time has expired, and I am saying as a nice compromise here that I suggest that we follow up with Mr. Markey's suggestion that if you would like to submit in writing to the chairman and the committee, and we will get this to Mr. Markey post haste. And thank you very much for your testimony. The committee is adjourned.

[Whereupon, at 1:03 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

INDIANA UNIVERSITY SCHOOL OF LAW—BLOOMINGTON
March 8, 2001

The Hon. CLIFF STEARNS
Chairman
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

DEAR CHAIRMAN STEARNS: Thank you once again for the opportunity to participate in the Subcommittee's March 1, 2001, hearing on Privacy in the Commercial World. It was a privilege to be invited, and I particularly appreciate your foresight in holding such an open and wide-ranging discussion of privacy issues, and your thoughtfulness and consideration when moderating the discussion.

We were asked during the hearing to respond in writing to two additional questions. First, you asked us to respond to Mr. Gordon's inquiry about the constitutional bounds of Congress' authority to legislate in the area of privacy. I attach a supplemental statement that attempts to do so.

Second, you referred to us Mr. Markey's request that we disclose any "on-going consulting contracts" to which we are parties. I am happy to reiterate what I said during the hearing: I have worked on privacy issues with many businesses, professional groups, associations, academic institutions, not-for-profit organizations, gov-

ernment agencies, think-tanks, and even a recent political campaign. My only ongoing consulting contract is with the Indianapolis law firm of Ice Miller, where I have served since 1997 as senior counsel for information law.

Finally, I am aware that the next privacy-related hearing before the Subcommittee concerns European privacy protections and their impact on consumers and businesses in Europe and the United States. Again, I applaud you for taking up this important subject, because I believe there has been considerable misunderstanding about how privacy law is actually applied within Europe, and regrettable inattention to the impact of European privacy law on European citizens. I would like to comment on four points in particular.

First, many of the requirements of the EU data protection directive have not been enforced. For example, the directive requires European nations to condition the collection, March 7, 2001 use, or transfer of personal information on "opt-in" consent. This is rarely done in practice. Privacy scholar Amitai Etzioni tells of regularly asking his European audiences if anyone has ever been asked to "opt-in." To date, Etzioni reports only one positive response—from a man who was asked for "opt-in" consent by Amazon.com, a U.S. company. "It seems that this EU directive is one of those laws that is enacted to keep one group—privacy advocates and their followers—happy and, as a rule, is not enforced so that commerce and life can continue." Amitai Etzioni, "Protecting Privacy," *Financial Times,* April 9, 1999, at 18.

A January 2001 study by Consumers International bears out Etzioni's conclusion. The study found that while U.S. and European Web sites collect personal information at nearly comparable rates (66 percent in the United States; 63 percent in Europe), U.S. sites provide *better* privacy protection, despite having no specific legal obligation to do so, than European sites, which are subject to comprehensive legal requirements. In fact, the study concluded: "US-based sites tended to set the standard for decent privacy policies." Consumers International, *Privacy@net: An International Comparative Study of Consumer Privacy on the Internet* at 6 (2001) (emphasis added).

A second observation is that when restrictive privacy rules actually have been enforced, for example, as part of national data protection laws that predated the directive, they have contributed to significant economic and social costs. The financial services sector provides some of the clearest examples. Restrictive national privacy laws have acted as a barrier to competition, giving the dominant incumbent a monopoly over the information it possesses about its customers, and denying new market entrants the information needed to provide and market financial services. As a result, financial services are provided by far fewer institutions—one-tenth the number that serve U.S. customers, despite the fact that the pan-European market has almost one and one-half times as many households. This means that European consumers have fewer choices of companies and services, fewer locations at which they can obtain financial services, and fewer ATMs—one-third the number in the United States—at which they can obtain and deposit funds.

Restrictive privacy laws also mean that consumers cannot take advantage of their complete credit histories, thereby restricting the mobility of consumers, because of the difficulty of obtaining credit from new institutions. As a result, economist Walter Kitchenman writes, in Europe "consumer lending is not common, and where it exists, it is concentrated among a few major banks in each country, each of which has it own large databases." Walter F. Kitchenman, *The European Union Directive on Privacy as a Barrier to Trade* (2000). In fact, European consumers, although they outnumber their U.S. counterparts, have access to one-third less credit as a percentage of gross domestic product. Moreover, the absence of standardized, complete consumer data reduces lender confidence and impedes the securitization and pooling of loans, thereby furthering limiting the availability of credit and driving up its price. Consumers also pay more for other financial services and products because of the lack of competition, the difficulty of obtaining service from another institution without a portable credit history, and the absence of other efficiencies made possible through information-sharing.

Third, if U.S. lawmakers don't hear loud complaints from European businesses about restrictive privacy laws, it likely reflects not only the limited extent to which at least the EU data protection directive is being enforced, but also the fact that many dominant companies welcome the anticompetitive impact of such laws. By keeping competitors out and making it harder for customers to take their business elsewhere, European privacy laws help dominant incumbents maintain their stranglehold on markets. In France, for example, the EU country with the strictest financial privacy laws, seven banks control more than 96 percent of banking assets. The seven dominant French banks already own extensive databases—they have no need to share information about their customers with anyone. And the fact that this system restrains innovation, hurts customer choice, and increases price is not a great

concern to those banks because the same system also restrains competition and makes it easier to hold customers and capital captive.

Finally, European and U.S. markets differ in many significant ways. The vast potential European market is, in fact, divided into many smaller markets by languages, cultures, and, at least until the euro is in widespread use, currencies. Moreover, the longstanding practical and legal restraints on the productive use of information have contributed to shaping radically different customer expectations in Europe than in the United States. For example, until recently, telephone bills in many EU countries did not include a listing of long-distance calls. Europeans just did not expect to have that type of tool for evaluating the accuracy of telephone charges. U.S. consumers, by contrast, have lengthy experience with expecting the businesses with which they deal to keep detailed call and charge records, so that the customer can verify that bills are accurate. And, of course, Europe does not have a "First Amendment" or a tradition of constitutional protection for information flows.

I mention these four points only to highlight the importance of your inquiry and the need for caution before attempting to emulate European-style privacy protection.

Thank you again both for the opportunity to participate in last week's hearing and for your foresight in carefully scrutinizing a wide range of issues about the current privacy debate, before attempting to reach any conclusion about whether further legislation is necessary or, if so, what the nature of that legislation may be. If I can be of any service, I hope you will not hesitate to contact me.

Yours sincerely,

FRED H. CATE
Professor of Law and Harry T. Ice Faculty Fellow

Enclosure

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

SUPPLEMENTAL STATEMENT OF PROFESSOR FRED H. CATE

Mr. Chairman: You asked the witnesses in the March 1, 20001, hearing on Privacy in the Commercial World to respond to Mr. Gordon's inquiry about the constitutional bounds of Congress' authority to legislate in the area of privacy. This statement attempts to do so.

I read the Constitution and the Supreme Court's jurisprudence as permitting Congress to legislate privacy protection only when it has a constitutional basis for doing so (in this case, the interstate commerce clause), and when that legislation meets the requirements of the First Amendment. First Amendment review is required of any law—privacy-related or otherwise—that limits the ability of individuals or nongovernmental institutions to engage in expression. That limit does not have to take the form of a direct prohibition to trigger First Amendment scrutiny, although most privacy laws have that effect.

Strict Scrutiny

Of course, not all restrictions on expression trigger the same type of First Amendment review. This point was largely obscured in last week's hearings, due perhaps to the fact that the Supreme Court's jurisprudence in this area is not always clear or consistent. As a general mater, however, direct government restraints, prior restraints, restraints based on the viewpoint of the expression or, in many cases, the content of the speech, require *strict scrutiny,* the highest form of scrutiny applied by the Court. Under this standard, which is the one that the Supreme Court has most frequently applied when reviewing privacy laws, the government bears the burden of showing that the law is (1) necessary to serve a compelling interest, and that the law (2) imposes no greater burden than is necessary to achieve that purpose. The need to evaluate both the purpose of the law and how narrowly it is tailored is why most of us at last week's hearing focused on what *harm* a privacy law is intended to prevent or remedy, and what cost or other burdens privacy law imposes on consumers and businesses. A privacy law that does not respond to a specific, significant harm will not be found to serve a compelling interest, and a law that imposes unnecessary costs, or costs in excess of the benefits it generates, will not be found to be the least restrictive means of achieving the government's interest. In either case, the Court would almost certainly strike down the law as unconstitutional. Moreover, it is important to reiterate that it is the *government's* responsibility under the First Amendment to demonstrate both the importance of the interest and the precision with which the law is tailored.

Intermediate Scrutiny

Although most privacy laws have been reviewed under strict scrutiny, not all have. Some courts have applied various forms of intermediate scrutiny, usually on the basis that the expression affected by the privacy law was *commercial* in nature. Although specific tests vary in detail, all intermediate scrutiny tests require that the government demonstrate that the law is intended to serve an important or substantial government interest, and that the law be narrowly tailored to achieving that interest. As you know, Professor Volokh testified, and I agree with him, that intermediate scrutiny was inappropriate for reviewing privacy laws and regulations because, even though the expression affected occurred in a commercial context, it was not "commercial speech" (i.e., it did not propose a commercial transaction). Some lower courts have nevertheless reviewed privacy laws or regulations under intermediate scrutiny. When they have done so, however, they have tended to find that the law or regulation failed even this level of scrutiny. In other words, they applied intermediate scrutiny because there was no need to apply strict scrutiny: The restriction being challenged could not survive even the lower standard of review.

The most recent example of this type of scrutiny was the decision of the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission.* The appellate court struck down the Commission's rules requiring that telephone companies obtain explicit consent from their customers before using data about those customers' calling patterns to market products or services to them.[1] The court found that the FCC's rules, by limiting the use of personal information when communicating with customers, restricted U.S. West's speech and therefore were subject to First Amendment review. Although the court applied intermediate scrutiny, it determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a "*specific and significant harm*" on individuals, and that the rules were "*. . . no more extensive than necessary to serve [the stated] interests . . .*"[2]

> Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm.[3]

The court found that for the Commission to demonstrate that the "opt-in" rules were sufficiently narrowly tailored, it must prove that less restrictive "opt-out" rules would not offer sufficient privacy protection, and it must do so with more than mere speculation:

> Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.[4]

The court found that the FCC had failed to show why burdensome "opt-in" rules were necessary, and therefore struck down the rules as unconstitutional. The Supreme Court declined to review the case.[5]

The Dominance of First Amendment Rights

The result in *U.S. West* is not surprising, because, whether analyzed under strict or intermediate scrutiny, privacy laws and regulations rarely survive constitutional review. For example, the Supreme Court has accorded privacy rights little protection when confronted with freedom of association claims of groups such as the American Communist Party.[6] The Supreme Court has struck has down ordinances that would require affirmative consent before receiving door-to-door solicitations,[7] before receiving Communist literature,[8] even before receiving "patently offensive" cable programming.[9] The words of the Court in the 1943 case of *Martin v. Struthers*—involving a local ordinance that banned door-to-door solicitations without explicit ("opt-in") householder consent—are particularly apt: "Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants."[10]

Similarly, the Court often has demonstrated little concern for the privacy interests of unwilling viewers or listeners, rejecting claims against broadcasts of radio programs in Washington, D.C. streetcars,[11] R-rated movies at a drive-in theater in Jacksonville, Florida,[12] and a jacket bearing the phrase "Fuck the Draft" worn in the corridors of the Los Angeles County Courthouse.[13] And plaintiffs rarely win suits brought against the press for disclosing private information. When information is true and obtained lawfully, the Supreme Court repeatedly has held that the state may not restrict its publication without first meeting strict scrutiny. Under this requirement, the Court has struck down laws restricting the publication of confidential government reports,[14] and of the names of judges under investigation,[15] juvenile suspects,[16] and rape victims.[17] Even if information published by the press is subsequently proved to be false, the Supreme Court has demonstrated extraordinary deference to First Amendment expression rights and little concern for the privacy interests involved.[18]

In fact, when privacy rights conflict with free expression rights before the Court, the latter prevail, virtually without exception. The dominance of the free expression rights over privacy interests is so great that Peter Edelman has written:

> [T]he Court [has] virtually extinguished privacy plaintiff's chances of recovery for injuries caused by truthful speech that violates their interest in nondisclosure . . . If the right to publish private information collides with an individual's right not to have that information published, the Court consistently subordinates the privacy interest to the free speech concerns.[19]

This is true irrespective of whether the speaker is an individual or an institution.

The Impact on Congress

So what does this mean for Congress? I believe it necessitates that *whenever* Congress restricts the flow of information in an effort to protect privacy it must demonstrate (1) what harms it is acting to prevent or remedy, (2) that such harms are serious enough to constitute a substantial or compelling government interest, (3) that the law is not broader, or does not regulate appreciably more expression, than is necessary to achieve that interest, and (4) that there are not other tools (such as technologies or market solutions) that would achieve the same end with less interference with information flows. The precise test (i.e., whether the interest must be "compelling" or "substantial" and whether the legislation must be the "least restrictive means" or merely "narrowly tailored" to achieve that interest) will depend upon the nature both of the expression restricted and of the legislation itself, but effectively *all* restrictions on the collection, use, or disclosure of information by the private sector will have to survive this basic First Amendment review.

This is a very high, but not impossible, burden. As a practical matter, it means that Congress cannot legislate to protect individuals from embarrassment or a "general level of discomfort" as a result of the disclosure of true information about them. It also means that Congress cannot broadly restrict uses of information that do not cause harm in an effort to target those that do.

On the other hand, the First Amendment does not restrict Congress from facilitating the creation and enforcement of private contracts. For example, Congress has broad discretion under the First Amendment to require disclosures, provided that those requirements do not interfere with expression to such an extent, or impose such high costs, that they constitute an unconstitutional restraint on expression. The Supreme Court has also found that Congress has significantly broader latitude to act to protect *children,* provided that the law is not so overbroad that it impinges on adult's expression. This explains why the Children's Online Privacy Protection Act may be constitutional under the First Amendment as applied to children, but similar restrictions would be unconstitutional if applied to adults. Moreover, Congress has broad—although not unlimited authority—to regulate the *government's* use of information (i.e., to require privacy policies on government Web sites, or to reduce the amount of personal information the government collects from citizens). Congress can fund the development of privacy protecting technologies (either directly or through tax incentives or other subsidies), and sponsor commissions or other research initiatives about privacy issues. Congress can help educate citizens about the steps that we—and often, only we—can take to protect our own privacy.

Conclusion

The First Amendment is often lamented as a regrettable restraint on the ability of Congress and other governmental bodies to act in the best interest of the citizenry and protect the public. It may sometimes have that effect. But I view it differently. The First Amendment reflects the fact that expression, and the information that is essential to expression, are so integral to our democracy and our economy, that laws affecting them always pose a great risk to citizens and consumers. Even

when motivated by the most noble of purposes, those laws can result in untold damage, especially if they are not precisely targeted. Moreover, laws regulating expression and information are often attractive to policymakers and to the public; such laws frequently respond to immediate concerns and they usually do not require the expenditure of taxpayer dollars.

The First Amendment reflects a constitutional calculation that because of the attractiveness of laws limiting expression and the great risks that they pose, the government should only be allowed to enact and enforce such laws when they are *necessary* to prevent or remedy a specific, significant *harm*, and when they are *closely tailored* to affect only that expression that causes the harm. Viewed in this light, the First Amendment does *not* limit Congress' authority to restrict expression when necessary to prevent substantial harms. It only limits Congress' authority to restrict expression when that restriction is not necessary or is designed to serve a less important purpose.

Notes

[1] U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 528 U.S. 1188 (2000).
[2] Id. at 1235 (quoting Rubin v. Coors Brewing Co., 514 U.S. 476, 486 (1995)) (emphasis added).
[3] Id. (emphasis added).
[4] Id. (emphasis added).
[5] U.S. West, Inc. v. Federal Communications Comm'n, 528 U.S. 1188 (2000).
[6] Communist Party of the U.S. v. Subversive Activities Control Board, 367 U.S. 1 (1961); Scales v. United States, 367 U.S. 203 (1961); Noto v. United States, 367 U.S. 290 (1961).
[7] Martin v. Struthers, 319 U.S. 141 (1943).
[8] Lamont v. Postmaster General, 381 U.S. 301 (1965).
[9] Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Comm'n, 518 U.S. 727 (1996).
[10] Martin v. Struthers, 319 U.S. at 141.
[11] Public Utilities Commission v. Pollack, 343 U.S. 451 (1952).
[12] Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975).
[13] Cohen v. California, 403 U.S. 15 (1971).
[14] New York Times Co. v. United States, 403 U.S. 713 (1971).
[15] Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978).
[16] Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).
[17] Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
[18] Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988); Time, Inc. v. Hill, 385 U.S. 374 (1952).
[19] Peter B. Edelman, "Free Press v. Privacy: Haunted by the Ghost of Justice Black," 68 *Texas Law Review* 1195, 1198 (1990).

RESPONSE FOR THE RECORD OF OF SOLVEIG SINGLETON, THE COMPETITIVE ENTERPRISE INSTITUTE

Question (1) Below I will summarize my view of the outer constitutional limits of Congressional action on privacy (noting, however, that the most Congress can do is probably not what Congress should do).

Opt-in. An opt-in regime is probably a violates of rights of free speech as applied to many cases, for it will in effect operate as a ban on the exchange of truthful information in many cases.

Opt-out. Opt-out is more likely to pass constitutional muster. There may be some contexts where opt-out is unconstitutional, for examples, if it restricts the use of information from public records. In addition, the Court might find, consistent with copyright cases, that it is inconsistent with free speech principles to create a property right in facts.

Default Contract Terms. Congress could clarify the default rules for a contract that is silent on the matter of privacy. This would not restrict speech, so long as companies remained free to set their own terms differently from the default.

Notice. Congress could require companies to give notice of their privacy practices.

Question (2) Below I offer information in response to the question about consulting clients and my work on privacy.

Some think tanks such as AEI and Brookings do permit industry consulting. But my former employer, the Cato Institute, for whom I worked when I first formed my views on privacy, has an explicit rule prohibiting consulting related to analysts' policy topics with interested for-profit companies or associations that represent for-profit companies. The Competitive Enterprise Institute, where I presently work, also assumes that such consulting is inappropriate. Thus I have never worked as an industry consultant on privacy or any other topic that I also work on in the policy world.

I have, worked as a consultant to a number of non-profit public policy groups on privacy. These groups are the Mackinaw Center, the Foundation for Economic Education (a small market-oriented group that works with students and academics), the National Center for Policy Analysis (a conservative group based in Texas), and the Democracy Online Task Force (meeting in Washington, D.C.). This is an all-inclusive list.